VŠB – Technická univerzita Ostrava

Fakulta strojní

Institut dopravy

Analýza požadavků na funkční bezpečnost vozidel

Requirement Analysis of Vehicles Functional Safety

Student: **Bc. Jaroslav Jelínek**

Vedoucí diplomové práce: **Ing. Jan FAMFULÍK, Ph.D.**

Ostrava 2011

VŠB - Technická univerzita Ostrava
Fakulta strojní
Institut dopravy

Zadání diplomové práce

Student:	**Bc. Jaroslav Jelínek**
Studijní program:	N2301 Strojní inženýrství
Studijní obor:	2301T003 Dopravní technika a technologie
Specializace:	10 Kolejová doprava
Téma:	Analýza požadavků na funkční bezpečnost vozidel Requirement Analysis of Vehicles Functional Safety

Zásady pro vypracování:

Cíl: Stanovit požadavky na integritu bezpečnosti konstrukčních skupin a subsystémů vybraného vozidla. U vybraného subsystému provést návrh jeho architektury a orientační výpočet.

Osnova:
1. Úvod
2. Popis principů používaných pro zajištění funkční bezpečnosti
3. Metody pro stanovení cílové míry poruch systémů souvisejících s funkční bezpečností
4. Analýza požadavků na integritu bezpečnosti konstrukčních skupin a subsystémů vybraného vozidla
5. Orientační výpočet cílové míry poruch vybraného subsystému
6. Závěr

Seznam doporučené odborné literatury:

1. ČSN EN 61508. Český normalizační institut. 2002
2. Daněk A., Široký J. Teorie obnovy dopravních prostředků. Ostrava: VŠB TU Ostrava. ISBN 80-7078-568-3
3. Famfulík J, Míková J, Krzyžanek R. Teorie údržby. Ostrava: VŠB TU Ostrava. 2007. ISBN 978-80-248-1509-1
4. ČSN EN 50 (191). Český normalizační institut. 1993

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Jan Famfulík, Ph.D.**

Datum zadání: 17.12.2010

Datum odevzdání: 23.05.2011

doc. Ing. Vladimír Smrž, Ph.D.
vedoucí katedry

prof. Ing. Radim Farana, CSc.
děkan fakulty

Poděkování patří Všem, kteří mi poskytli při vypracování této diplomové práce pomocné rady, informace, materiály a předali řadu svých osobních zkušeností v zadané problematice.

Velké poděkování bych chtěl vyjádřit hlavně vedoucímu mé diplomové práce, panu Ing. Janu Famfulíkovi, Ph.D.

.

Místopřísežné prohlášení studenta

Prohlašuji, že jsem celou diplomovou práci včetně příloh vypracoval samostatně pod vedením vedoucího diplomové práce a uvedl jsem všechny použité podklady a literaturu.

V Ostravě …… ……

podpis studenta

Prohlašuji, že

- jsem byl seznámen s tím, že na moji diplomovou práci se plně vztahuje Zákon č. 121/2000 Sb. – autorský zákon, zejména §35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo.

- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen„VŠB-TUO“) má právo nevýdělečně ke své vnitřní potřebě diplomovou práci užít (§35 odst. 3).

- souhlasím s tím, že jeden výtisk diplomové práce bude v elektronické podobě uložena v Ústřední knihovně VŠB-TUO k nahlédnutí a jeden výtisk bude uložen u vedoucího diplomové práce. Souhlasím s tím, že údaje o diplomové práci budou zveřejněny v informačním systému VŠB-TUO.

- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít toto dílo v rozsahu §12 odst. 4 autorského zákona.

- bylo sjednáno, že užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

- beru na vědomí, že odevzdáním své práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, bez ohledu na výsledek její obhajoby.

V Ostravě: ……

……

podpis

Jméno a příjmení autora práce: Jaroslav Jelínek

Adresa trvalého pobytu autora práce: Kosmická 1562, Ostrava, 708 00.

ANOTACE DIPLOMOVÉ PRÁCE

Jelínek, J.: Analýza požadavků na funkční bezpečnost vozidel: diplomová práce. Ostrava: VŠB – Technická univerzita Ostrava, Fakulta strojní, Institut dopravy, 2011, 85 s. Vedoucí práce: Famfulík, J.

Diplomová práce se zabývá analýzou požadavků na funkční bezpečnost vozidel. V úvodní části se zabývá obecným popisem principů používaných pro zajištění bezpečnosti a metodami pro stanovení cílové míry poruch systémů, které souvisí s funkční bezpečností. Následuje analýza požadavků na integritu bezpečnosti konstrukčních skupin a subsystémů na vybrané vozidlo. V poslední části je proveden orientační výpočet cílové míry poruch vybraného subsystému vozidla a jeho vyhodnocení s určením funkční bezpečnosti.

ANNOTATION OF MASTER THESIS

Jelínek, J.: Requirement Analysis of Vehicles Functional Safety: Master Thesis. Ostrava: VŠB - Technical University of Ostrava, Faculty of Mechanical Engineering, Institute of Transport, 2011, 85 p. Thesis head: Famfulík, J.

Master thesis is dealing with analysis of requirements for vehicles functional safety. The introduction part describes general principles used for ensuring security and methods used for determining the target failure of systems which are related to functional safety. The following part analyzes requirements for safety integrity assemblies and subsystems of the selected vehicle. In the last part is created approximate calculation of the target failure of the selected subsystem and its evaluation specifying functional safety.

Obsah diplomové práce

Seznam použitých zkratek a symbolů

ALARP	„nejnižší rozumně proveditelný“
BF	bezpečnostní funkce
C	následek nebezpečné události
CAN	datová sběrnice
ČSN	česká státní norma
DC	diagnostické pokrytí
E/E/PE	elektrické a/nebo elektronické a/nebo programovatelné elektronické
EN	evropská norma
EUC	řízené zařízení
F	četnost a doba vystavení v nebezpečné oblasti
f	četnost nebezpečné události bez systémů souvisejících s bezpečností
F_{np}	četnost vyžádání ochranného systému, jež souvisí s bezpečností
F_p	četnost rizika za přítomnosti ochranných prostředků
F_t	četnost přípustného rizika
FTA	strom poruchových stavů
HFT	odolnost proti vadám hardwaru
IEC	Mezinárodní úřad pro elektrotechniku
MTTR	střední doba do zotavení
MooN	architektura M z N kanálů
N	dusík
P	možnost vyhnout se nebezpečné události
PFD	průměrná pravděpodobnost poruchy při vyžádání
PFD_{avg}	střední pravděpodobnost poruchy při vyžádání ochranného systému souvisejícího s bezpečností
PFD_{FE}	průměrná pravděpodobnost poruchy při vyžádání pro subsystém koncových prvků
PFH_G	průměrná pravděpodobnost poruchy při vyžádání pro skupinu kanálů s majoritní rozhodovací logikou
PFD_{Gi}	průměrná pravděpodobnost poruchy při vyžádání pro každou rozhodovací skupinu senzorů
PFD_{Gj}	průměrná pravděpodobnost poruchy při vyžádání pro každou rozhodovací skupinu koncových prvků
PFD_{SYS}	průměrná pravděpodobnost poruchy při vyžádání bezpečnostní funkce pro E/E/PE systém související s bezpečností
PFD_{SYSp}	průměrná pravděpodobnost poruchy prvku při vyžádání bezpečnostní funkce pro E/E/PE systém související s bezpečností

PFH_G	pravděpodobnost poruchy za hodinu pro skupinu kanálů s majoritní rozhodovací logikou
PFH_{SYS}	pravděpodobnost poruchy za hodinu pro E/E/PE systém související s bezpečností
R	riziko bez systémů souvisejících s bezpečností
SIL	úroveň integrity bezpečnosti
SIS	bezpečnostní přístrojový systém
SW	software
T_1	kontrolní interval periodické zkoušky
t_{CE}	ekvivalentní střední doba prostoje kanálu
W	pravděpodobnost nežádoucího výskytu
λ	intenzita poruch kanálu v subsystému
λ_D	intenzita nebezpečných poruch
λ_{DD}	intenzita nebezpečných zjištěných poruch
λ_{DU}	intenzita nebezpečných nezjištěných poruch
ΔR	nutné snížení rizika

1 Úvod

Funkční bezpečnost je součástí celkové bezpečnosti, která závisí na správných reakcích procesu, nebo vybraných zařízení a zajišťují jejich bezpečnost. Pojmem, funkční bezpečnosti se zabývá norma ČSN EN 61 508 a je mezinárodně uznávaným standardem pro zařízení, která využívají E/E/PE systémy zaručující bezpečnost. Norma je všeobecná a neomezuje se pouze na sektor strojních zařízení. Tato norma byla použita jako hlavní zdroj při vypracovávání této práce.

Posuzování rizika je to velice užitečný proces, díky kterému je možno získat velmi důležité informace, které dále pomáhají rozhodnout od způsobu, kterým bude dosaženo bezpečnosti daného zařízení.

Analýza rizika umožňuje určit nebezpečné situace a stanovit bezpečnostní funkce pro požadovanou integritu bezpečnosti. Aplikací normy ČSN EN 61 508 se snižují pravděpodobnosti poruch a nedostatků ve všech životních fází daného zařízení.

Tato práce obsahuje vysvětlení pojmů spojených s bezpečností, které jsou důležité pro pochopení funkční bezpečnosti. Je zde ukázáno několik metod, které slouží ke stanovení úrovně integrity bezpečnosti.

Dosažené poznatky z oblasti bezpečnosti jsou aplikovány na vybraný subsystém zvoleného vozidla. Pro aplikaci jsem volil městský autobus od firmy Solaris Urbíno 15 provozovaný Dopravním podnikem Ostrava a. s., u kterého je mi známo jeho konstrukční řešení a funkce nainstalovaných bezpečnostních zařízení. Vybraný subsystém je tvořen hnacím spalovacím motorem značky DAF, předehřívacím naftovým zařízením od firmy Eberspächer, systémem na potlačení požáru od firmy Foogmaker a zařízením na detekci kouře v prostoru pro přepravované osoby.

Cílem práce je u tohoto subsystému stanovit s pomocí normy ČSN EN 61 508 požadavky na integritu bezpečnosti tohoto subsystému. Po přiřazení integrity bezpečnosti vybraných systémů provedu návrh bezpečnostní funkce a orientační výpočet pravděpodobnosti nebezpečné poruchy při vyžádání bezpečnostní funkce.

2 Principy používané pro zajištění funkční bezpečnosti

Základní principy pro zajištění funkční bezpečnosti zařízení vychází z normy ČSN EN 61 508, která představuje mezinárodně uznávaný bezpečnostní standart pro zajištění funkční bezpečnosti. Tato norma je sice omezena na zařízení, kde jsou využívány E/E/PE systémy, které zaručují bezpečnost, ale současně nachází plné využití i u posuzování systémů založených na jiných technologických principech.

K pochopení těchto principů je nutno se seznámit se zněním některých základních definicí funkční bezpečnosti, které obsahuje tato norma [1].

Norma ČSN EN 61 508 se skládá ze sedmi částí:

Část 1: Všeobecné požadavky,
Část 2: Požadavky na E/E/EP systémy související s bezpečností,
Část 3: Požadavky na software,
Část 4: Definice a zkratky,
Část 5: Příklady metod určování úrovní integrity bezpečnosti,
Část 6: Metodické pokyny pro použití IEC 61 508 - 2 a IEC 61 508 - 3,
Část 7: Přehled technik a opatření.

2.1 Základní terminologie používaná v souladu s funkční bezpečností

V přehledu terminologie jsou uvedené pouze ty pojmy, které usnadňují pochopení principů funkční bezpečnosti nebo se vyskytují v této práci.

2.1.1 Termíny týkající se bezpečnosti

- nebezpečí: potenciální zdroj poškození,
- nebezpečná událost: nebezpečná situace, jejímž výsledkem je poškození,
- riziko: kombinace pravděpodobnosti výskytu poškození a závažnosti tohoto poškození,
- přípustné riziko: riziko, které je přijatelné v daných souvislostech založených na běžných hodnotách společnosti,
- zbytkové riziko: riziko, které zůstává po přijetí ochranných opatření,
- bezpečnost: nepřítomnost nepřijatelného rizika,

- funkční bezpečnost: část celkové bezpečnosti týkající se EUC a systému řízení EUC závislá na správném fungování E/E/PE systémů souvisejících z bezpečností,
- bezpečný stav - stav EUC, při kterém je dosaženo bezpečnosti [4].

2.1.2 Termíny pro systémy - všeobecná hlediska

- systém: soubor prvků, které na sebe podle návrhů vzájemně působí, kde prvkem systému může být další systém, označovaná jako subsystém, který může být systémem řídícím nebo řízeným,
- architektura: specifické uspořádání hardwarových a softwarových prvků v systému,
- modul: diskrétní součástka nebo funkční soubor uzavřených standardních programů nebo diskrétních součástek patřících k sobě,
- kanál: prvek nebo skupina prvků provádějící nezávisle danou funkci,
- diverzita: různé prostředky pro realizaci požadované funkce,
- redundance: existence dalších prostředků, kromě prostředků, které by mohly být u dané funkční jednotky dostačující pro plnění požadované funkce [4].

2.1.3 Termíny pro systémy z hlediska týkajícího se bezpečnosti

- systém související z bezpečností: navržený systém, který provádí požadované bezpečnostní funkce nezbytné pro dosažení nebo udržení bezpečného stavu u EUC a je určen pro zajišťování potřebné integrity bezpečnosti u požadované bezpečnostní funkce,
- jednoduchý E/E/PE systém související s bezpečností: systém, u kterého jsou dobře definovány režimy poruchy každé jednotlivé součásti, a lze plně určit chování systému v podmínkách poruchového stavu,
- systém související z bezpečností: navržený systém, který provádí požadované bezpečnostní funkce nezbytné pro dosažení nebo udržení bezpečného stavu u EUC a je určen pro zajišťování potřebné integrity bezpečnosti u požadované bezpečnostní funkce,
- jednoduchý E/E/PE systém související s bezpečností: systém, u kterého jsou dobře definovány režimy poruchy každé jednotlivé součásti, a lze plně určit chování systému v podmínkách poruchového stavu [4].

2.1.4 Termíny pro bezpečnostní funkce a integritu bezpečnosti

- bezpečnostní funkce: funkce, která má být realizována E/E/PE systémem souvisejícím s bezpečností a která je určena pro zajištění nebo udržení bezpečného stavu EUC z hlediska konkrétní nebezpečné události,
- integrita bezpečnosti: pravděpodobnost systému souvisejícího z bezpečností uspokojivě plnit požadované bezpečnostní funkce za všech stanovených podmínek a po stanovenou dobu,
- integrita bezpečnosti hardwaru: část integrity bezpečnosti systémů souvisejících s bezpečností týkajících se náhodných poruch hardwaru v nebezpečném režimu poruchy,
- úroveň integrity bezpečnosti (SIL): diskrétní úroveň (jedna ze čtyř možných) pro stanovení požadavků integrity bezpečnosti bezpečnostních funkcí přiřazených E/E/PE systémům souvisejícím s bezpečností, kde úroveň integrity bezpečnosti čtyři má nejvyšší úroveň integrity bezpečnosti a úroveň jedna nejnižší,
- specifikace bezpečnostních požadavků: specifikace obsahující všechny požadavky na bezpečnostní funkce, které musí systém související z bezpečností plnit,
- specifikace požadavků bezpečnostních funkcí: specifikace obsahující požadavky na bezpečnostní funkce, které musí systémy související s bezpečností plnit,
- specifikace požadavků integrity bezpečnosti: specifikace obsahující požadavky integrity bezpečnosti bezpečnostních funkcí, které musí systémy související s bezpečností plnit,
- režim provozu: zamýšlený způsob využití systému souvisejícího s bezpečností z hlediska četnosti jeho vyžádání,
- režim provozu s nízkým vyžádáním: bezpečnostní funkci předchází zásah jiného bezpečnostního systému,
- režim s vysokým nebo trvalým vyžádáním: bezpečnostní funkce je jedinou ochranou systému,
- cílová míra poruch: předpokládaná pravděpodobnost režimu nebezpečné poruchy, které má být dosaženo z hlediska požadavků stanovené integrity bezpečnosti,
- střední hodnotou pravděpodobností poruchy během provádění dané funkce (u režimu provozu s nízkým vyžádáním),
- pravděpodobností nebezpečné poruchy za hodinu (u režimu provozu s vysokým nebo trvalým vyžádáním),

- nutné snížení rizika: snížení rizika, kterého má být dosaženo E/E/PE systémy souvisejícími s bezpečností založenými na jiných technických principech a vnějšími prostředky pro snížení rizika tak, aby se zajistilo nepřekročení přípustného rizika [4].

2.1.5 Termíny pro vadu, poruchu a chybu

- vada, závada, poruchový stav: abnormální podmínka, která může způsobit snížení nebo ztrátu způsobilosti funkční jednotky plnit požadovanou funkci,
- předcházení vadám: použití technik a postupů, jejichž cílem je se zamezit vnášení vad během všech fází životního cyklu,
- odolnost proti vadám: schopnost funkční jednotky pokračovat v plnění požadované funkce i za přítomnosti vad nebo chyb,
- porucha, selhání: ukončení schopnosti funkční jednotky plnit požadovanou funkci,
- systematická porucha: porucha, kterou jednoznačně způsobila určitá příčina a kterou je možné odstranit změnou konstrukce nebo výrobního procesu, provozních postupů nebo dokumentace
- nebezpečná porucha: porucha, která je schopna uvést systém související s bezpečností do nebezpečného stavu nebo stavu, v němž není schopna plnit svou funkci,
- závislá, podmíněná porucha: porucha, jejíž pravděpodobnost nelze vyjádřit jako jednoduchý součin nepodmíněných pravděpodobností jednotlivých událostí, které ji vyvolaly $\left(P(AaB) > P(A) \cdot P(B)\right)$,
- společná porucha: porucha, která má za následek poruchu systému a která je výsledkem jedné nebo více událostí, které způsobily současné poruchy dvou nebo více samostatných kanálů u vícekanálového systému,
- chyba: nesoulad mezi počítanou, pozorovanou nebo teoreticky správnou hodnotou,
- lidská chyba, omyl: lidská činnost vyvolávající nezamýšlený výsledek [4].

2.1.6 Termíny pro potvrzení míry bezpečnosti

- odhad funkční bezpečnosti: zkoumání, založené na důkazu, za účelem posouzení funkční bezpečnosti dosažené jedním nebo více E/E/EP systémy souvisejícími s bezpečností nebo vnějšími prostředky pro snížení rizika,
- prověrka funkční bezpečnosti: systematické a nezávislé zkoumání, jehož cílem je stanovení, zda postupy charakteristické pro požadavky funkční bezpečnosti

jsou v souladu s plánovanými záměry a zda jsou tyto záměry účinně realizovány a jsou vhodné pro dosažení stanovených cílů,

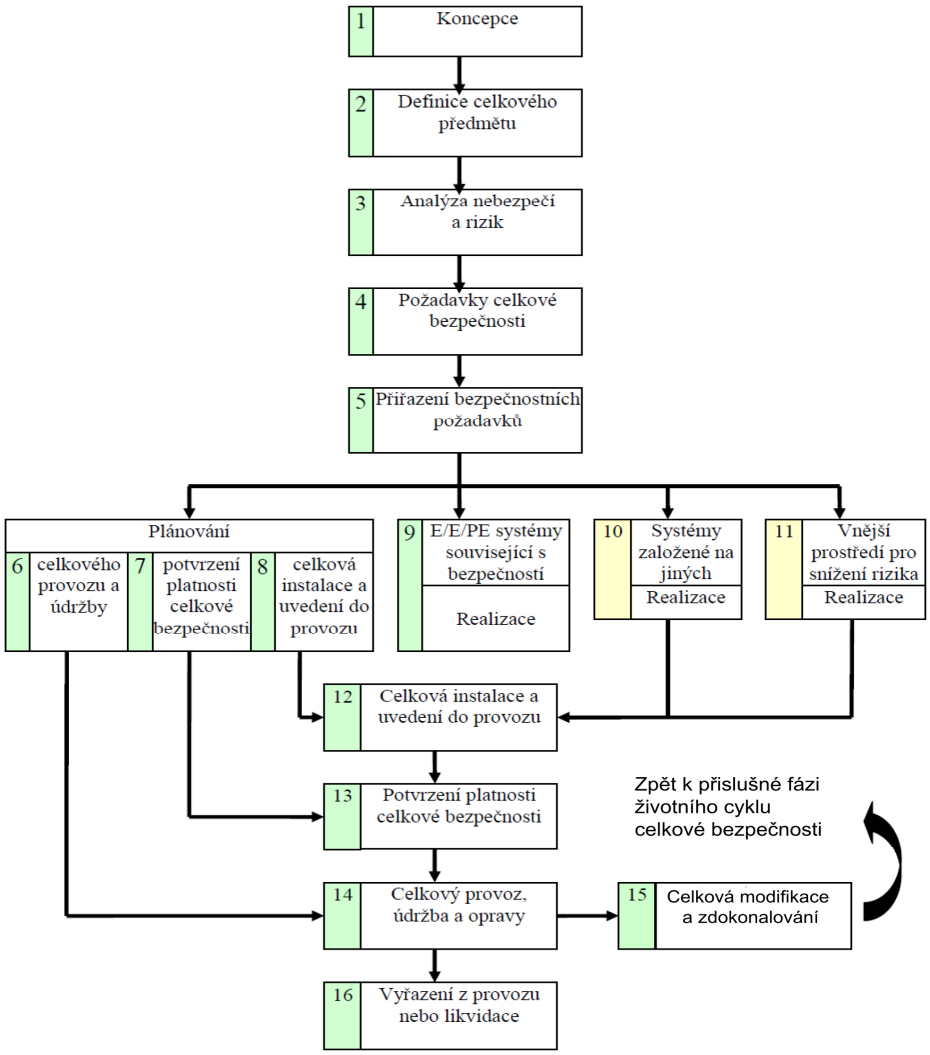
- diagnostické pokrytí je podíl na snížení pravděpodobnosti nebezpečných poruch hardwaru v důsledku provádění diagnostických testů [4].

2.2 Požadavky životního cyklu celkové bezpečnosti

Životní cyklus celkové bezpečnosti zahrnuje tato opatření pro snížení rizika:

- E/E/PE systémy související s bezpečností,
- systémy související s bezpečností založené na jiných technologických postupech,
- vnější prostředky pro snížení rizika [1].

Na obrázku č. 1 je systematické rozčlenění na fáze životního cyklu celkové bezpečnosti, které jsou podstatné pro dosažení požadované funkční bezpečnosti E/E/EP systémů.



Obrázek č. 1: Životní cyklus celkové bezpečnosti [1]

Tento životní cyklus je nutné použít jako základ pro uplatňování shody s normou ČSN EN 61 508. Při použití jiného cyklu celkové bezpečnosti se musí tento cyklus stanovit při plánování funkční bezpečnosti a při tom musí být splněny všechny cíle a požadavky normy [1].

2.2.1 Koncept

Ve fázi konceptu se musí stanovit potencionální zdroje nebezpečí a získat informace o stanovených nebezpečích jako je například korozívnost, toxicita, nebo podmínky výbuchu. Dále je nutné přihlédnout k nebezpečí v důsledku interakce s jinými EUC, které jsou již instalované nebo plánované [1].

2.2.2 Vymezení oblasti použití

Cílem je vymezení hranic EUC a systému řízeni EUC a stanovení předmětu analýzy nebezpečí a rizik. Musí se zde specifikovat fyzické zařízení včetně EUC a systému řízení EUC, které bude předmětem analýzy nebezpečí a rizik a stanovit vnější události, s kterými je třeba počítat v analýze nebezpečí a rizik [1].

2.2.3 Analýza nebezpečí a rizik

Nutné je určení nebezpečí a nebezpečných událostí pro všechny rozumně předvídatelné okolnosti, včetně poruchových podmínek a nesprávného použiti, stanovení sledu událostí vedoucích k nebezpečným událostem a určením rizik EUC, které jsou s nebezpečnými událostmi spojeny. Musí se zvážit opatřeni pro odstranění těchto nebezpečí a určit nebezpečí a nebezpečné události EUC i v systému řízení EUC za všech rozumě předvídatelných okolností. Musí se vyhodnotit pravděpodobnost nebezpečných události a určit potenciální důsledky spojené s těmito událostmi. Pro každou určenou nebezpečnou událost se musí vyhodnotit nebo odhadnout riziko EUC.

2.2.4 Požadavky celkové bezpečnosti

Pro každé určené nebezpečí se musí určit bezpečností funkce nutné pro zajištění požadované funkční bezpečnosti. Ty musí byt součástí specifikace požadavků celkových bezpečnostních funkcí. Pro každou nebezpečnou událost se musí stanovit nutné sníženi rizika. Sníženi rizika muže být určeno kvantitativním nebo kvalitativním způsobem. Pro každou bezpečnostní funkci se musí stanovit požadavky integrity bezpečnosti z hlediska nutného snížení rizika. Ty musí tvořit příslušnou specifikaci požadavků celkové integrity bezpečnosti.

2.2.5 Přiřazení bezpečnostních požadavků

Prvním cílem je přirazeni bezpečnostních funkci ze specifikace požadavku celkové bezpečnosti a přirazení úrovně integrity bezpečnosti každé bezpečnostní funkci. Je nutno specifikovat navrhované systémy související s bezpečností, které se mají pro dosažení požadované funkční bezpečnosti použít. Nutného snížení rizika je možné dosáhnout prostřednictvím vnějších prostředků pro snížení rizika

Každá bezpečnostní funkce se musí přiřadit k jednotlivým navrhovaným E/E/PE systémům souvisejícím s bezpečností při respektování snížení rizik zajišťovaných systémy souvisejícími s bezpečnosti založenými na jiných technických principech a vnějšími prostředky pro snížení rizika tak, aby se u dané bezpečnostní funkce dosáhlo nutného snížení rizika. Při zjištění, že nutného snížení rizika nelze dosáhnout, přiřazováním opakujícím se procesem, musí se daná architektura modifikovat a přiřazení se musí opakovat.

Požadavky integrity bezpečnosti pro každou bezpečnostní funkci se musí posoudit, aby se zjistilo, zda každý parametr silové integrity bezpečnosti při střední pravděpodobnosti poruchy dokáže plnit při vyžádání svou projektovanou funkci (u režimu provozu s nízkým vyžádáním) nebo splňuje požadavek pravděpodobnosti nebezpečné poruchy za hodinu (u režimu provozu s vysokým nebo nepřetržitým vyžádáním).

Tabulka č. 1: Úroveň integrity pro režim provozu s nízkým vyžádáním [1]

Úroveň integrity bezpečnosti (SIL)	Stření pravděpodobnost poruchy plnit svou navrženou funkci na vyžádání
4	$\geq 10^{-5}$ až $<10^{-4}$
3	$\geq 10^{-4}$ až $<10^{-3}$
2	$\geq 10^{-3}$ až $<10^{-2}$
1	$\geq 10^{-2}$ až $<10^{-1}$

Přiřazení musí pokračovat s vážením možnosti společných poruch, které by mohly vést k nebezpečnému režimu poruchy všech systémů. Předvídatelné poruchy nesmí ovlivňovat redundantní systémy související s bezpečností ani vnější prostředky pro snížení rizika. V případě že přiřazení už dostatečně pokročilo, musí se stanovit požadavky integrity bezpečnosti každé bezpečnostní funkci přiřazené E/E/PE systému souvisejícímu

s bezpečností a to z hlediska úrovně integrity bezpečnosti podle tabulek č. 2 a č. 3. Musí se určit, zda parametrem cílové integrity bezpečnosti je střední pravděpodobnost poruchy plnit při vyžádání projektovanou funkci nebo pravděpodobnost nebezpečné poruchy za hodinu.

Tabulka č. 2: Úroveň integrity pro režim provozu s vysokým vyžádáním [1]

Úroveň integrity bezpečnosti (SIL)	Pravděpodobnost nebezpečné poruchy za hodinu
4	$\geq 10^{-9}$ až $<10^{-8}$
3	$\geq 10^{-8}$ až $<10^{-7}$
2	$\geq 10^{-7}$ až $<10^{-6}$
1	$\geq 10^{-6}$ až $<10^{-5}$

Norma stanovuje dolní mez pro cílové míry poruch v režimu nebezpečné poruchy, které lze vyžadovat. Číselné hodnoty v tabulce se považují za mez, kterou lze v současné době dosáhnout u relativně složitých systému.

Žádnému jednotlivému E/E/PE systému souvisejícímu s bezpečností nesmí být přidělena cílová míra poruch integrity bezpečnosti nižší než hodnota uvedena v tabulkách č. 2 a č. 3 [1].

2.2.6 Plánování celkového provozu a údržby

Plány provozu a údržby E/E/PE systému související s bezpečností musí být sestaveny tak, aby během provozu a údržby bylo zajištěno udržení požadované funkční bezpečnosti. Musí se připravit plán, který musí obsahovat a určovat běžné preventivní činnosti, které se musí provádět pro udržení požadované funkční bezpečnosti.

2.2.7 Potvrzení platnosti celkové bezpečnosti

Všechna zařízení použitá pro kvantitativní měření, která jsou součástí potvrzování platnosti, musí být kalibrovaná podle specifikace s návazností na národní normu, nebo specifikaci prodeje. Při neshodách mezi očekávanými a skutečnými výsledky se provede analýza, která rozhodne, zda se bude v potvrzování platnosti pokračovat, nebo se přejde zpět k předchozí části potvrzování platnosti [1].

2.2.8 Celkový provoz, údržby o opravy

Celkový provoz, údržby a opravy je nutno zajistit tak, aby bylo zajištěno udržování požadované funkční bezpečnosti. Je nutno zpracovat plán údržby systému, postupy pro provoz údržby a opravy systému a postupy pro provoz a údržbu softwaru

2.2.9 Celková modifikace a zdokonalování

Modifikace a zdokonalování má zajistit přijatelnou funkční bezpečnost jak v průběhu, tak i po realizaci modifikační nebo zdokonalovací fáze. Všechny modifikace ovlivňující funkční bezpečnost musí vyvolat návrat zpět k příslušné fázi životního cyklu celkové bezpečnosti. Potom musí proběhnout všechny následné fáze podle platných postupů pro tyto fáze [1].

2.2.10 Vyřazení z provozů nebo likvidace

Před vyřazením z provozu nebo likvidací se musí vypracovat plán, který musí obsahovat postupy pro ukončení provozu a demontáže stávajícího systému.

2.3 Nutné snížení rizika

Je takové snížení rizika, kterého se musí dosáhnout pro dosažení přípustného rizika v konkrétní situaci. Účelem stanovení přijatelného rizika určité nebezpečné události je vyjádření toho, co se považuje za přijatelné jak z hlediska četnosti nebo pravděpodobnosti nebezpečné události, tak jejich vlastních následků. Systémy související s bezpečností se navrhují tak, aby snížily četnost nebo pravděpodobnost nebezpečné události, popřípadě následky nebezpečné události. Při určování toho, co bude představovat toto přijatelné riziko u konkrétní aplikace tvořit, je třeba vzít v úvahu několik vstupů:

- metodické pokyny příslušného bezpečnostního regulačního orgánu,

- jednání a dohody s různými stranami, které se na dané aplikaci podílejí,

- průmyslové normy a metodické pokyny,

- názory od nezávislých průmyslových expertních a vědeckých poradních orgánů [5].

2.3.1 Integrita bezpečnosti

Je pravděpodobnost systému souvisejícího s bezpečností uspokojivě plnit požadované bezpečnostní funkce po stanovenou dobu za všech stanovených podmínek. Týká se vlastností systémů souvisejících s bezpečností provádět bezpečnostní funkce.

Integritu bezpečnosti budou tvořit dva následující prvky:

- integrita bezpečnosti hardwaru:

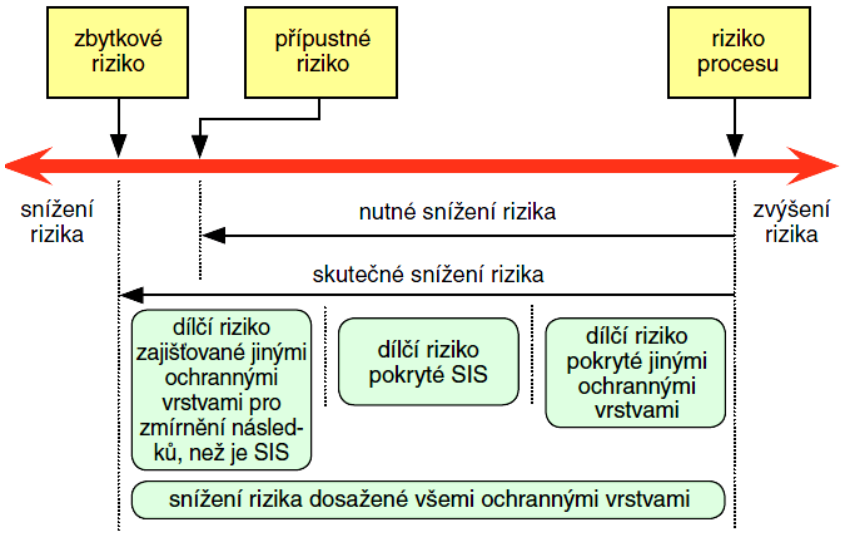
Část integrity bezpečnosti, která souvisí s náhodnými poruchami v režimu nebezpečných poruch. Dosažení stanovené úrovně integrity bezpečnosti lze s přijatelnou přesností odhadnout a proto je možné použitím běžných pravidel pro operace s pravděpodobnostmi požadavky rozdělit mezi jednotlivé subsystémy. Dosažení dostatečné integrity může být nutné použití redundantních architektur.

- systematická integrita bezpečnosti:

Část integrity bezpečnosti, která souvisí se systematickými poruchami v režimu nebezpečných poruch. Přestože může být možné odhadnout střední intenzity poruch v důsledku systematických poruch z údajů o poruchách získaných z vad návrhu a společných poruch vyplývá, že rozdělení poruch je těžko předvídatelné.

Důsledkem je zvýšení nejistoty ve výpočtech pravděpodobnosti poruch v konkrétních situacích. Pro minimalizování této nejistoty je nutně třeba posouzení provádět při zvolení nejlepších technik je nutno si uvědomit, že to nemusí být nutně ten případ, kdy opatření pro ztížení pravděpodobnosti náhodné poruchy hardwaru budou mít odpovídající vliv i na pravděpodobnost systematické poruchy.

Požadovaná integrita bezpečnosti E/E/PE systému založených na jiných technických principech nebo vnějších prostředků pro snížení rizika musí mít takovou úroveň, aby zajistila, že četnost poruch systému je dostatečně malá, aby zabránila tomu, že četnost nebezpečných událostí překročí hodnotu požadovanou pro splnění přípustného rizika a systémy související s bezpečností upraví následky poruch na rozsah požadovaný ke splnění přípustného rizika [5].



Obrázek č. 2: Snížení rizika [10]

Obecný model předpokládá existenci EUC a systému řízení EUC, existenci problému spojených s lidským činitelem a bezpečnostní ochrana zařízení zahrnující vnější prostředky pro snížení rizika,E/E/PE systémy související s bezpečností a systémy související s bezpečností založené na jiných technických principech.

Nutného snížení rizika se dosahuje kombinací všech ochranných prostředků. Nutné snížení rizika potřebné pro dosažení stanoveného přípustného rizika je od výchozího bodu rizika EUC zobrazeno na obrázku číslo 2 [10].

2.3.2 Riziko a integrita bezpečnosti

Je důležité, aby byl jasně vymezen a vyjasněn rozdíl mezi rizikem a integritou bezpečnosti. Riziko je míra pravděpodobnosti a následek výskytu stanovené nebezpečné události. To lze pro různé situace ohodnotit. Přípustné riziko se stanovuje na určitém společenském základě a vyžaduje zvážení společenských a politických činitelů.

Integrity bezpečnosti se používá jedině u E/E/PE systému souvisejících s bezpečností a systému souvisejících s bezpečností založených na jiných technických principech a vnějších prostředků pro snížení rizika a je mírou pravděpodobnosti těchto systémů, prostředků uspokojivě dosahovat nutného snížení rizika z hlediska stanovených bezpečnostních funkcí. Pro stanovení přípustného rizika a provedení odhadu nutného snížení rizika je možné systémům souvisejícím s bezpečností přiřadit požadavky integrity bezpečnosti [5].

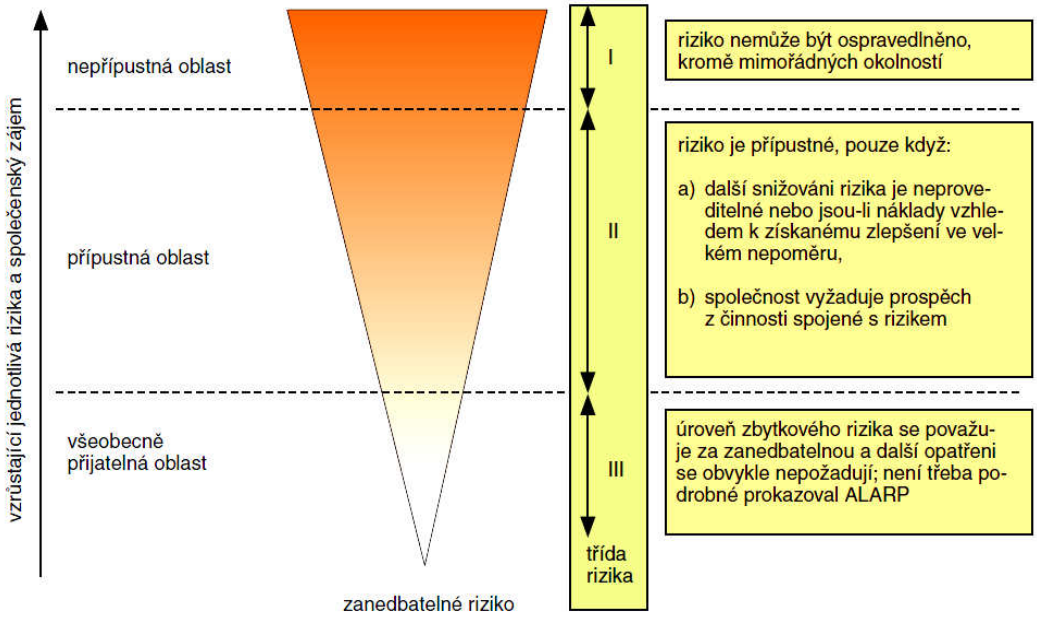
3 Metody pro stanovení cílové míry poruch systémů souvisejících s funkční bezpečností

Existuje několik postupů, kterými jsme schopni stanovit analýzu rizik pro konkrétní řešenou úlohu. Výběr metody závisí na složitosti řešené úlohy, povaze rizika a požadované úrovní snížení tohoto rizika. Ve složitých případech je nutno volit i více než jednu metodu a to hlavně v případech, kdy kvalitativní metodou byla přiřazena integrita bezpečnosti SIL 4. V tomto případě musíme použít kvantitativní metodu, která přináší konkrétní číselné hodnoty.

3.1 Koncepce ALARP

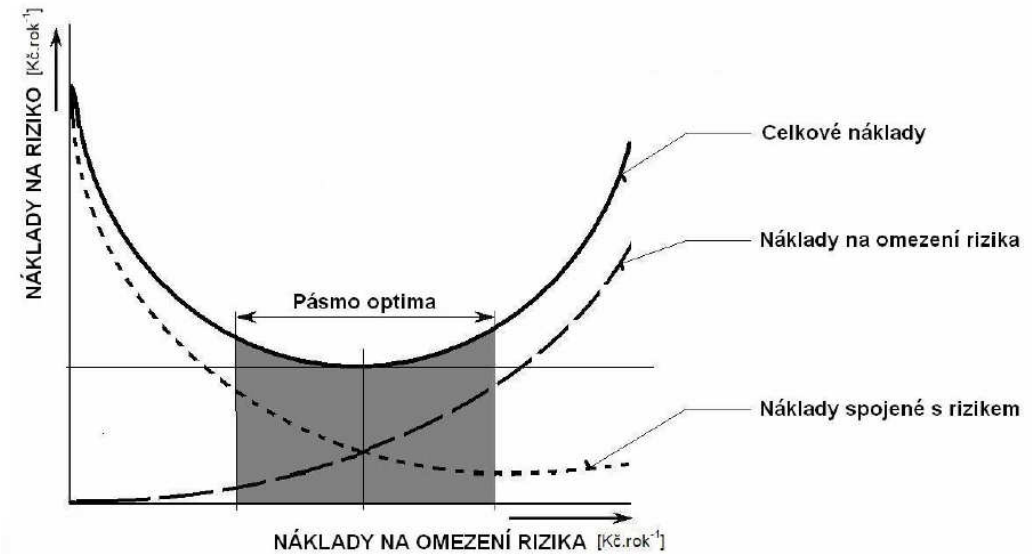
Hlavní zkoušky používané při určení průmyslových rizik patří i stanovení toho, zda je dané riziko tak veliké, že se musí zcela vyloučit, nebo je riziko tak malé, že bude bezvýznamné. Nachází li se riziko někde mezi těmito dvěma stavy je nutno přihlédnout na přínosy plynoucí z přijetí tohoto rizika a zvážit náklady na jeho další snížení a současně zajistit, aby bylo riziko sníženo na nejnižší možnou úroveň.

Princip ALARP vyžaduje snížení jakéhokoliv rizika na co nejnižší možnou úroveň, nebo na co nejnižší rozumě proveditelnou úroveň. Je-li riziko někde mezi těmito dvěma extrémy potom je výsledné riziko u konkrétní aplikace rizikem přípustný. Tato tří pásmová metoda je na obrázku číslo 3 [10].



Obrázek č. 3: Přípustné riziko a ALARP [10]

Nad určitou úrovní se riziko požaduje za nepřípustné a za všech běžných okolností ho nelze ospravedlnit. Pod touto úrovní je přípustná oblast, kde je provádění daných činností dovoleno za předpokladu, že s nimi spojená rizika byla snížená na co nejnižší rozumně proveditelnou úroveň. Přípustné se tady liší od přijatelného tím, že vyznačuje ochotu žít s rizikem za účelem získání určitého prospěchu, a současně očekávající udržení tohoto rizika pod kontrolou a jeho snížení, v případě, že to lze provést.



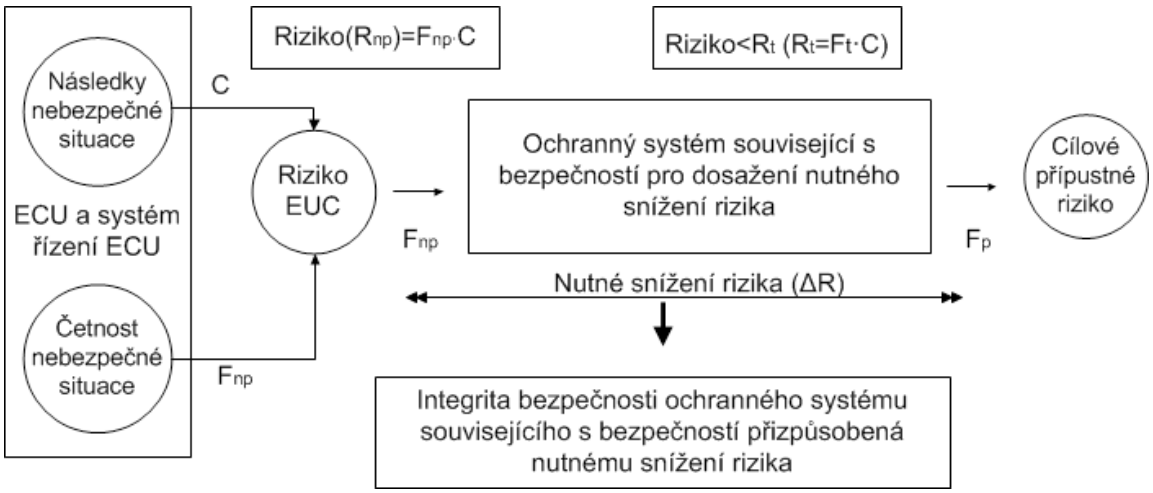
Obrázek č. 4: Optimální pásmo při nákladech na odstranění rizika [10]

U vyššího rizika se doporučuje očekávat i úměrně vyšší náklady na jeho snížení. Tam, kde rizika nejsou tak důležitá, je třeba úměrně tomu vynaložit nižší náklady na jejich snížení a v dolní části přípustné oblasti bude dostačující určitá vyváženost mezi náklady a přínosy [10].

Pod přípustnou oblastí se úrovně rizika považují za tak bezvýznamné, že regulátor nepožaduje jejich další snížení. Je to všeobecně přijatelná oblast, kde jsou rizika, ve srovnání s riziky, které všichni denně zažíváme malá. V této obecně přijatelné oblasti nejsou sice nutné žádné jednotlivé činnosti pro prokazování ALARP, ale je třeba věnovat trvalou pozornost tomu, aby se riziko na této určené úrovni udrželo [5].

3.2 Určení úrovní integrity bezpečnosti:kvantitativní metoda

Kvantitativní metoda dává konkrétní hodnotu v případě stanovení přípustného rizika v číselném vyjádření za předpokladu stanovení číselných cílů úrovní integrity bezpečnosti. Obecný model použitý pro ilustraci obecných principů je model zobrazen na obrázku č. 5.



Obrázek č. 5: Přiřazení integrity bezpečnosti pomocí kvantitativní metody [5]

Hlavní kroky metody:

- určení přípustného rizika z tabulky,

- určení rizika EUC,

- určení nutného snížení rizika pro dosažení přípustného rizika,

-přiřazení nutného snížení rizika E/E/PE systémům souvisejícím s bezpečností a systémů založených na jiných technických principech a vnějším prostředkům pro snížení rizika.

Četnost spojenou s rizikem existujícím u EUC včetně rizika plynoucího z lidského činitele a systému řízení EUC bez jakýchkoliv ochranných prostředků lze odhadnout použitím kvantitativních metod odhadu rizika. Tato četnost, s níž by se nebezpečná událost mohla vyskytovat bez jakýchkoliv ochranných prostředků, je jedna ze dvou složek rizika EUC. Druhou složkou je následek nebezpečné události [5].

Četnost vyžádání ochranného systému F_{np} je možno stanovit:

- analýzou intenzity poruch ze srovnatelných situací,

- na základě dat z příslušných bází dat,

- výpočtem využívajícím vhodných předpovědních metod.

Příklad výpočtů [5]:

$$PFD_{avg} \leq \frac{F_t}{F_{np}} \left[-\right] \tag{1}$$

$$PFD_{avg} = \frac{F_t}{F_{np}} = \Delta R \left[-\right] \tag{2}$$

PFD_{avg} - střední pravděpodobnost poruchy při vyžádání ochranného systému souvisejícího s bezpečností, která je mírou poruch integrity bezpečnosti ochranného systému souvisejícího s bezpečností režimu s nízkým vyžádáním $\left[-\right]$

F_t - četnost přípustného rizika $\left[-\right]$

F_{np} - četnost vyžádání ochranného systému souvisejícího s bezpečností $\left[-\right]$

F_p - četnost rizika za přítomnosti ochranných prostředků $\left[-\right]$

ΔR - nutné snížení rizika $\left[-\right]$

Určení F_{np} pro EUC je důležité kvůli jeho vztahu k PFD_{avg} a tím k úrovni integrity bezpečnosti ochranného systému souvisejícího s bezpečností. Nutnými kroky pro dosažení úrovně integrity bezpečnosti v situaci, kdy se celého nutného snížení rizika dosahuje jediným ochranným systémem souvisejícím s bezpečností, který musí snížit četnost rizika minimálně z F_{np} na F_p.

Je nutné určení četnosti rizika EUC bez přidání jakýchkoliv ochranných prostředků, určení následku C bez přidání jakýchkoliv ochranných prostředků a určení pravděpodobnosti poruchy při vyžádání ochranného bezpečnostního systému [5].

3.3 Určení úrovní integrity bezpečnosti-kvalitativní metoda: diagram rizika

Při přijetí kvalitativní metody se pro zjednodušení zavádí několik parametrů, které dohromady charakterizují základní vlastnosti nebezpečné situace v případě selhání nebo nedostupnosti systémů souvisejících s bezpečností.

Z každého ze čtyř souborů se vybere jeden parametr a takto vybrané parametry se potom vzájemně kombinují pro rozhodnutí o tom, jaká úroveň integrity bezpečnosti se systémům souvisejícím s bezpečností přiřadí.

3.3.1 Systém diagramu rizika

Zjednodušený postup je založen na rovnici [5]:

$$R = f \cdot C \ [-] \tag{3}$$

R - riziko bez systémů souvisejících s bezpečností $[-]$

f - četnost nebezpečné události bez systémů souvisejících s bezpečností $[-]$

C - následek nebezpečné události $[-]$

Četnost nebezpečné události F se v tomto případě považuje za četnost, kterou tvoří tři ovlivňující činitelé:

- četnost a doba vystavení v nebezpečné oblasti,

- možnost se nebezpečné události vyhnout,

- pravděpodobnost nežádoucího výskytu.

To vede k těmto čtyřem parametrům rizika [5]:

- následku nebezpečné události (C),

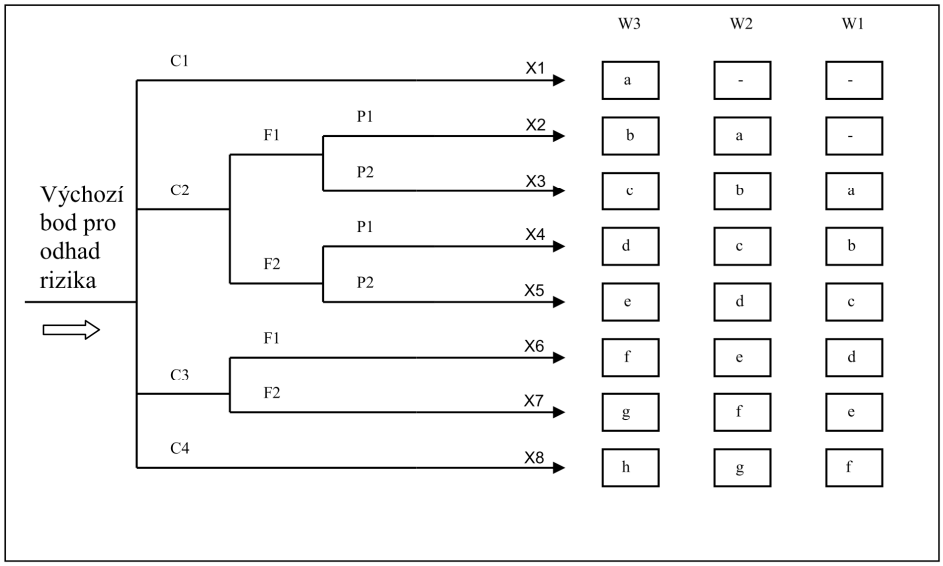
- četnosti a době vystavení v nebezpečné oblasti (F),

- možnosti se nebezpečné události vyhnout (P),

- pravděpodobnosti nežádoucího výskytu (W).

3.3.2 Provedení diagramů rizika pro obecné schéma

Kombinací parametrů rizika C, F, P a W umožňuje vytvořit diagram rizika jaký je zobrazen na obrázku č. 6.



Obrázek č. 6: Diagram rizika k určení integrity bezpečnosti [5]

Použití parametrů rizika C, Fa P vede na několik výstupů X1,X2,X3 až X8. Každý z těchto výstupů je směrován do jedné ze tří stupnic W1,W2 nebo W3. Každý stupeň těchto stupnic vyznačuje nutnou integritu bezpečnosti, kterou musí uvažovaný E/E/PE systém související s bezpečností splňovat,

Usměrňování do W1, W2 nebo W3 dovoluje přispět i dalším opatřením pro snížení rizika. Posouvání stupnic u parametrů W1, W2 a W3 je nutné z důvodu možnosti tří různých úrovní snížení rizika zajišťovaných dalšími opatřeními. Stupnice W3 poskytuje minimální snížení rizika zajišťované od jiných opatření. Stupnice W2 poskytuje střední minimální snížení rizika a stupnice W1 maximální snížení rizika.

Pro výstup diagramu rizika X1, X2 nebo X8 a pro konkrétní stupnici W1, W2 nebo W3 dává koncový výstup diagramu rizika určení úrovně integrity bezpečnosti E/E/PE systému souvisejícího s bezpečností o hodnotě 1, 2, 3 nebo 4 a u daného systému je mírou požadovaného snížení rizika. Toto snížení spolu s dalšími sníženími rizika získanými od jiných opatření a zohledněním stupnic W, dává nutné snížení rizika pro danou konkrétní situaci [5].

Tabulka č. 3: Vazba mezi nutným minimálním snížením rizika a SIL [5]

Nutné minimální snížení rizika	Úroveň integrity bezpečnosti
-	Žádné bezpečnostní požadavky
a	Žádné speciální bezpečnostní požadavky
b, c	1
d	2
e, f	3
g	4
h	Jeden E/E/PES systém související s bezpečností není dostačující

Tabulka č. 4: Údaje pro sestavení diagramu rizika [10]

Rizikový parametr		Klasifikace	Poznámky
Následek (C)	C1 C2 C3 C4	Menší zranění Zranění jedné nebo více osob s trvalými následky, smrt jedné osoby. Smrt několika osob. Smrt velkého počtu osob.	Systém klasifikace vytvořený pro posuzování zranění nebo smrti osob. Pro hodnocení materiálních škod nebo škod na životním prostředí je třeba vytvořit jiná klasifikační schémata.
Četnost a doba vystavení v nebezpečné oblasti (F)	F1 F2	Vzácné až častější vystavení v nebezpečné oblasti Časté až trvalé vystavení v nebezpečné oblasti	Parametr bere v úvahu četnost a dobu, po kterou jsou osoby vystaveny nebezpečí.
Možnost se nebezpečné události vyhnout (P)	P1 P2	Možné za určitých podmínek Téměř nemožné	Tento parametr zohledňuje: -provoz procesu, -rychlost vzniku události, -snadnost rozpoznání nebezpečí, -vyhnutí se nebezpečné události, -skutečná bezpečnostní zkušenost.
Pravděpodobnost nežádoucího výskytu (W)	W1 W2 W3	Velmi malá pravděpodobnost, že dojde k nežádoucím výskytům a je pravděpodobných pouze několik nežádoucích výskytů. Malá pravděpodobnost, že dojde k nežádoucím výskytům a pravděpodobných je málo nežádoucích výskytů. Poměrně vysoká pravděpodobnost, že dojde k nežádoucím výskytům a časté nežádoucí výskyty jsou pravděpodobné	Účelem činitele W je odhad četnosti nežádoucího výskytu bez přiznání jakýchkoliv systémů souvisejících s bezpečností, ale včetně všech vnějších prostředků pro snížení rizika

3.4 Určení úrovní integrity bezpečnosti - kvalitativní metoda: matice závažnosti nebezpečných událostí

Číselnou metodu určení integrity bezpečnosti není možné použít tam, kde nelze riziko kvalifikovat.

Konstrukce matice je založena na těchto požadavcích:

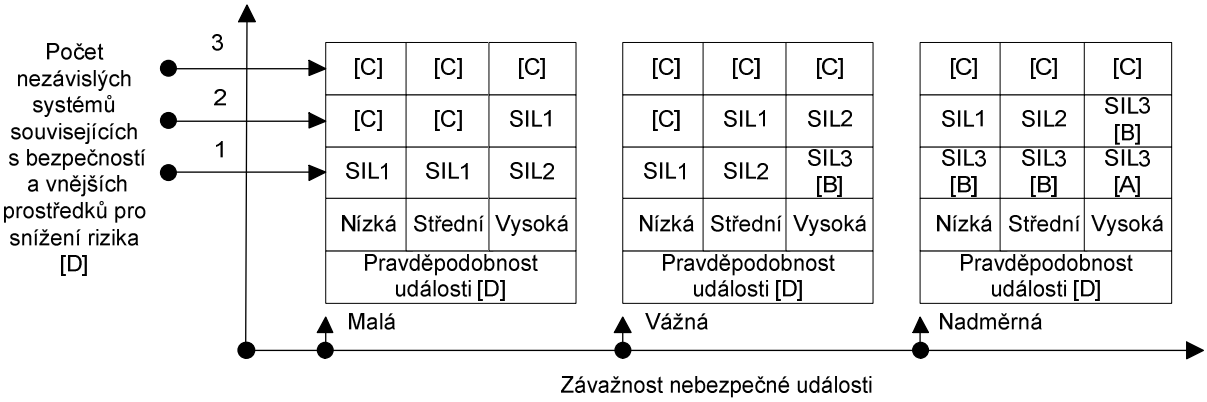
- systémy související s bezpečností jsou spolu s vnějšími prostředky pro snížení rizika nezávislé,

- každý systém související s bezpečností a vnější prostředky pro snížení rizika se považují za ochranné vrstvy, které poskytují vlastní dílčí snížení rizika,

- přidáním jedné ochranné vrstvy se zvyšuje integrita bezpečnosti o 1 stupeň,

- použije se pouze jeden E/E/PE systém související s bezpečností u kterého se touto metodou zjišťuje nutná úroveň integrity bezpečnosti [5].

Tyto uvedené požadavky vedou k matici závažnosti nebezpečných událostí ukázané na obrázku č. 7. Údaje uvedené v této matici jsou pouze pro pochopení všeobecných principů [5].



Obrázek č. 7: Matice závažnosti nebezpečných událostí [5]

[A] Jeden E/E/PE systém související s bezpečnosti s SIL3 nezajišťuje na této úrovni rizika a jeho dostatečné snížení jsou nutná přídavná opatření pro snížení rizika.

[B] Jeden E/E/PE systém související s bezpečností SIL3 nezajišťuje na této úrovni rizika jeho dostatečné snížení. Pro stanovení, zda jsou nutná přídavná opatření pro snížení rizika, je požadováno provedení analýzy nebezpečí a rizik.

[C] Není pravděpodobně požadování nezávislého E/E/PE systému souvisejícího s bezpečností.

[D] Pravděpodobnost události je pravděpodobnost, že k nebezpečné události dojde bez jakýchkoliv systému souvisejících s bezpečnosti nebo vnějších prostředků pro snížení rizika [5].

3.5 Požadavky životního cyklu bezpečnosti E/E/PE systému

V požadavcích životního cyklu je systematické rozčlenění na ty fáze životního cyklu, s kterými je třeba pro zajištění požadované funkční bezpečnosti E/E/PE systému souvisejících s bezpečnosti počítat a zdokumentovat všechny informace pro funkční bezpečnost E/E/PE systému souvisejících s bezpečností a to během celého životního cyklu bezpečnosti E/E/PE systému [2].

3.5.1 Návrh a vývoj E/E/PE systému

Návrh E/E/PE systému musí být takový, aby splnil všechny z následujících požadavků:

- omezení architektury na integritu bezpečnosti hardwaru,

- nepravděpodobnost nebezpečných náhodných poruch hardwaru,

- požadavky na předcházení poruchám a řízení systémových vad,

- na chování systému při zjištění vad [2].

3.5.2 Omezení architektury na integritu bezpečnosti hardwaru

Nejvyšší úroveň integrity bezpečnosti, kterou lze pro bezpečnostní funkci uplatňovat je omezena odolností proti vadám hardwaru a podílem bezpečných poruch subsystémů, které tuto bezpečnostní funkci realizují.

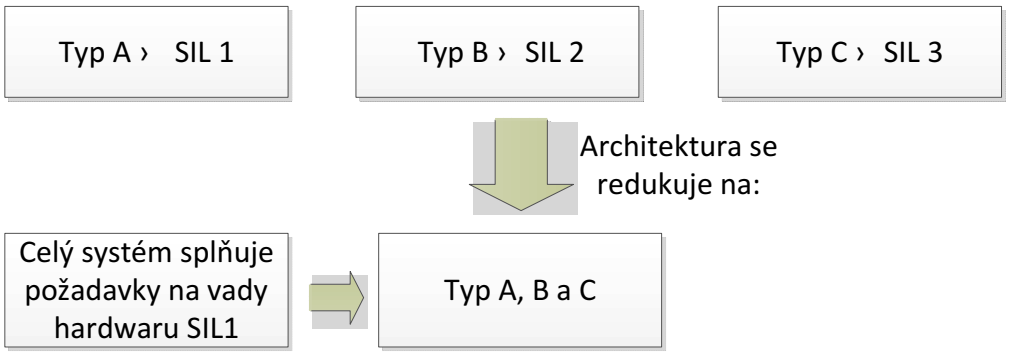
Z hlediska těchto požadavků platí že:

- odolnost proti vadám hardwaru N znamená, že N+1 vad by mohlo způsobit ztrátu dané bezpečnostní funkce. Při určování odolnosti proti vadám se nesmí brát v úvahu další opatření, které mohou účinky vad řídit jako je například diagnostika,

- kde jedna vada vede k přímo k výskytu jedné nebo více následných vad a ty se považují za vadu jedinou,

- při určování odolnosti proti vadám hardwaru je možné určité vady vynechat za předpokladu že pravděpodobnost jejich výskytu je vzhledem k požadavkům integrity bezpečnosti subsystému velmi malá,

- podíl bezpečných poruch podsystému je definován jako poměr střední intenzity bezpečných poruch a zjištěných nebezpečných poruch subsystému k celkové střední intenzitě poruch subsystému [2].



Obrázek č. 8: Příklad omezení integrity bezpečnosti pro jednokanálovou bezpečnostní funkci [2]

Subsystém typ A:

- jsou dobře definovány poruchové režimy jednotlivých složek,

- lze plně určit chování subsystému v podmínkách poruchových stavů,

- jsou k dispozici dostatečně spolehlivé údaje o poruchách získané provozu,

- jsou splněny požadované intenzity poruch pro zjištěné a nezjištěné poruchy [2].

Tabulka č. 5: Omezení architektury na subsystémy typu A [2]

Poměr bezpečných poruch	Odolnost proti vadám hardwaru		
	0	1	2
< 60%	SIL 1	SIL 2	SIL 3
60% - < 90%	SIL 2	SIL 3	SIL 4
90% - < 99%	SIL 3	SIL 4	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

Subsystém typ B:

- není dobře definován poruchový režim alespoň jedné ze složek, které tuto součást tvoří,

- nelze plně určit chování subsystému v podmínkách poruchových stavů,

- nejsou k dispozici dostatečně spolehlivé údaje o poruchách získané z provozu potvrzující tvrzení o intenzitě poruch pro zjištěné a nezjištěné nebezpečné poruchy,

- E/E/PE systému souvisejících s bezpečností kde je bezpečnostní funkce realizovaná prostřednictvím jednoho kanálu, zobrazeno na obrázku č. 8, musí být maximální úroveň integrity bezpečnosti hardwaru, kterou lze pro uvažovanou bezpečnostní funkci uplatňovat, určená subsystémem, který splnil požadavky nejnižší úrovně integrity bezpečnosti hardwaru [2].

Tabulka č. 6: Omezení architektury na subsystémy typu B [2]

Poměr bezpečných poruch	Odolnost proti vadám hardwaru		
	0	1	2
< 60%	Nedovolena	SIL 1	SIL 2
60% - < 90%	SIL 1	SIL 2	SIL 3
90% - < 99%	SIL 2	SIL 3	SIL 4
≥ 99%	SIL 3	SIL 4	SIL 4

3.5.3 Požadavky na odhad pravděpodobnosti poruchy bezpečnostní funkce v důsledku náhodných poruch hardwaru

Při odhadu pravděpodobnosti poruchy každé jednotlivé bezpečnostní funkce v důsledku náhodných poruch hardwaru se musí vzít v úvahu:

- architektura E/E/PE systému souvisejícího s bezpečností, protože souvisí s každou uvažovanou bezpečnostní funkcí,

- odhadnuté integrity poruch každého subsystému ve všech režimech, které by mohly vyvolat neztečnou poruchu systému souvisejícího s bezpečností, ale zjištěné diagnostickými testy,

- odhadnuté intenzity poruch každého subsystému ve všech režimech, ale nezjištěné diagnostickými testy,

- náchylnost E/E/PE systému na společné poruchy,

- diagnostické pokrytí diagnostickými testy a interval diagnostických testů,

- intervaly v nichž se provádějí periodické testy pro zajišťování nebezpečných vad nezjištěných diagnostickými testy,

- dobou opravy u zjištěných poruch,

- pravděpodobnost nezjištěné poruchy jakéhokoliv datového komunikačního procesu.

Interval diagnostických testů jakéhokoliv subsystému, jehož odolnost proti vadám hardwaru je větší než nula, musí být takový, aby umožnil E/E/PE systému souvisejícímu s bezpečností plnění požadavku pravděpodobnosti náhodné poruchy hardwaru. Interval diagnostických testů jakéhokoliv subsystému, jehož odolnost proti vadám hardwaru je roven nule, u kterého je bezpečnostní funkce zcela závislá na subsystému a který realizuje bezpečnostní funkci pracující v režimu s nízkým vyžádáním, musí být takový, aby umožnil systému splnění požadavků náhodné poruchy hardwaru [2].

3.5.4 Požadavky na chování systému při zjištění vady

Zjištění nebezpečné vady v jakémkoliv subsystému, jehož odolnost proti vadám hardwaru je větší než nula, musí mít za následek:

-stanovenou činnost pro dosažení nebo udržení bezpečného stavu,

-oddělení vadné části subsystému tak aby mohl pokračovat bezpečný provoz EUC, zatímco je vadná část opravena.

V případě že se oprava nedokončí v rámci střední doby do obnovy předpokládané ve výpočtu pravděpodobnosti náhodné poruchy hardwaru, potom musí být provedena činnost stanovená pro dosažení nebo udržení bezpečného stavu.

Zjištění nebezpečné poruchy v jakémkoliv subsystému, který má 0 odolnost proti vadám hardwaru a u něhož je bezpečnostní funkce zcela závislá a v případě, že tento subsystém používá pouze bezpečnostní funkce pracující v režimu s malým vyžádáním, musí mít za následek:

- stanovenou činnost pro dosažení nebo udržení bezpečného stavu,

- opravu vadného subsystému v rámci střední doby do obnovy předpokládané ve výpočtu pravděpodobnosti náhodné poruchy hardwaru. Během této doby musí být zajištěno trvání bezpečnosti EUC doplňkovými opatřeními a omezeními,

- snížení rizika zajišťované prostřednictvím opatření a omezení musí být alespoň stejné jako omezení rizika zajišťované E/E/PE systémem souvisejícím s bezpečností bez jakýchkoliv vad [2].

3.6 Hodnocení pravděpodobnosti poruchy hardwaru

Pro analýzu integrity bezpečnosti E/E/PE systému souvisejících s bezpečností je k dispozici několik metod. Nejobvyklejší jsou bezporuchové blokové schémata a Markovské modely obě tyto metody dávají při svém použití dobře výsledky, ale v případě složitých programovatelných elektronických subsystémů může být v porovnání s Markovskými modely určitá ztráta přesnosti při použití bezporuchovostního blokového schématu. Tam, kde porucha systému EUC vyžaduje zásah E/E/PE systému závisí pravděpodobnost výskytu nebezpečné události také na pravděpodobnosti poruchy systému řízení EUC. Existence takových poruch by mohla v případě jejich nesprávného hodnocení, vést k vyššímu než očekávanému zbytkovému riziku [6].

Výpočty jsou založeny na těchto předpokladech:

- u intenzity poruch součástí jsou během života systému konstantní,

- všechny kanály ve skupině kanálu mají stejné intenzity poruch i stejné diagnostické pokrytí,

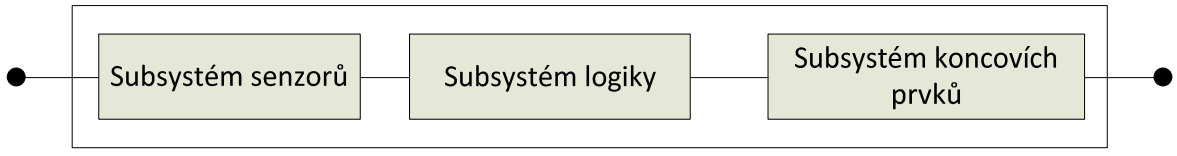
- celková intenzita poruch hardwaru kanálu subsystému je součet intenzity nebezpečných poruch a intenzity bezpečných poruch daného kanálu, u kterých se předpokládá, že jsou stejné,

- každá bezpečnostní funkce má dokonalé kontrolní periodické zkoušení a opravu,

- interval kontrolní zkoušky je o řád vyšší než interval diagnostické zkoušky [6].

3.6.1 Průměrná pravděpodobnost poruchy při vyžádání – režim provozu s nízkým vyžádáním

Průměrná pravděpodobnost poruchy při vyžádání bezpečnostní funkce se u E/E/PE systému určí výpočtem a kombinaci průměrné pravděpodobnosti poruchy při vyžádání pro všechny subsystémy, které společně tuto bezpečnostní funkci zajišťují.



Obrázek č. 9: Struktura subsystémů [6]

Vzorec pro výpočet [6]:

$$PFD_{SYS} = PFD_S + PFD_L + PFD_{FE} \quad [-] \tag{4}$$

PFD_{SYS} - průměrná pravděpodobnost poruchy při vyžádání bezpečnostní funkce pro E/E/PE systém související s bezpečností $[-]$

PFD_S - průměrná pravděpodobnost poruchy při vyžádání pro subsystém senzorů $[-]$

PFD_L - průměrná pravděpodobnost poruchy při vyžádání pro subsystém logiky $[-]$

PFD_{FE} - průměrná pravděpodobnost poruchy při vyžádání pro subsystém koncových prvků $[-]$

Při určování průměrné pravděpodobnosti poruchy při vyžádání každého subsystému se doporučuje dodržet u každého podsystému následující postup:

- nakreslit blokové schéma znázorňující součásti subsystému vstupních senzorů, součástí subsystému logiky nebo součástí subsystému koncových prvků,

- z tabulek uvedených v normě ČSN EN 61 508-6 určit pro šesti měsíční, jednoleté, dvouleté a desetileté intervaly periodických zkoušek,

- z tabulek uvedených v normě ČSN EN 61 508-6 odečíst průměrnou pravděpodobnost poruchy při vyžádání pro danou rozhodovací skupinu,

-v případě že bezpečnostní funkce závisí na více než jedné rozhodovací skupině souborů nebo akčních členů, jsou kombinované průměrné pravděpodobnosti poruchy při vyžádání subsystému senzorů nebo koncových prků, PFD_S nebo PFD_{FE}, daný těmito rovnicemi [6]:

$$PFD_S = \sum_i PFD_{Gi} \quad [-] \tag{5}$$

PFD_S - pravděpodobnost poruchy při vyžádání pro subsystém senzorů $[-]$

PFD_{Gi} - průměrná pravděpodobnost poruchy při vyžádání pro každou rozhodovací skupinu senzorů $[-]$

$$PFD_{FE} = \sum_{j} PFD_{Gj} \; [-] \tag{6}$$

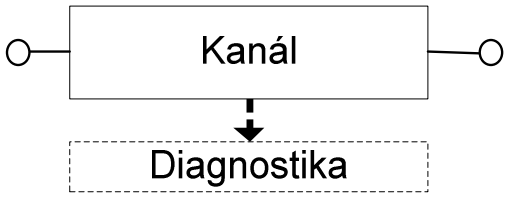
PFD_{FE} - průměrná pravděpodobnost poruchy při vyžádání pro subsystém koncových prvků $[-]$

PFD_{Gj} - průměrná pravděpodobnost poruchy při vyžádání pro každou rozhodovací skupinu koncových prvků $[-]$

3.6.2 Architektury pro režim provozu s nízkým vyžádáním

Architektura 1oo1 pro režim s nízkým vyžádáním

Tuto architekturu tvoří jediný kanál, kde jakákoliv nebezpečná porucha znamená při vzniku vyžádání poruchu bezpečnostní funkce.



Obrázek č. 10: Blokové schéma provedení 1oo1 [6]

Intenzita nebezpečných poruch λ_D [6]:

$$\lambda_D = \lambda_{DU} + \lambda_{DD} = \frac{\lambda}{2} \; [h] \tag{7}$$

λ_{DU} – intenzita nezjištěných nebezpečných poruch $[h]$

λ_{DD} – intenzita zjištěných nebezpečných poruch $[h]$

Ekvivalentní střední doba poruchy kanálů t_{CE} [6]:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \ \ [h] \tag{8}$$

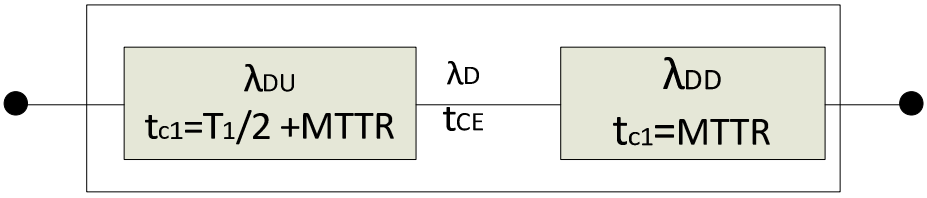
λ_{DU} - intenzita nebezpečných nezjištěných poruch $[h]$

λ_D - intenzita nebezpečných poruch $[h]$

λ_{DD} - intenzita zjištěných nebezpečných poruch $[h]$

T_1 - interval kontrolní (periodické) zkoušky $[h]$

$MTTR$ - střední doba do zotavení $[h]$



Obrázek č. 11: Blokové schéma bezporuchovosti 1oo1 [6]

Intenzita zjištěných poruch λ_{DU} [6]:

$$\lambda_{DU} = \frac{\lambda}{2} \cdot (1 - DC) \ [h] \tag{9}$$

λ - intenzita poruch v kanálu subsystému $[h]$

DC - diagnostické pokrytí $[-]$

Intenzita nezjištěných poruch λ_{DD} [6]**:**

$$\lambda_{DD} = \frac{\lambda}{2} \cdot DC \left[h\right] \tag{10}$$

λ - intenzita poruch v kanálu subsystému $\left[h\right]$

DC - diagnostické pokrytí $\left[-\right]$

Ekvivalentní střední doba prostoje kanálů PFD [6] :

$$PFD = 1 - e^{-\lambda_D \cdot t_{CE}} \left[-\right] \tag{11}$$

λ_D – intenzita nebezpečných poruch $\left[h\right]$

t_{CE} – ekvivalentní střední doba prostoje kanálu $\left[h\right]$

Architektura 1oo2 pro režim s nízkým vyžádáním

Architektura je tvořena dvěma paralelně spojenými kanály. Danou bezpečnostní funkci může zpracovat každý z této dvojice kanálů. V této architektuře by při vyžádání bezpečnostní funkce musela nastat porucha v obou kanálech.

Blokové schéma je vyobrazeno na obrázku č. 10 a č. 11. Pro výpočet t_{CE} používáme rovnici (8). U této architektury se předpokládá, že diagnostické testování zaznamená pouze zjištěné vady a nezmění žádné výstupní stavy [6].

3.6.3 Průměrná pravděpodobnost poruchy při vyžádání pro režim provozu s vysokým nebo nepřetržitým vyžádáním

Metoda výpočtu pravděpodobnosti poruchy bezpečnostní funkce u E/E/PE systému pracujícího v režimu s vysokým nebo nepřetržitým vyžádáním je stejná jako metoda výpočtu pro režim s nízkým vyžádáním pouze s tím rozdílem, že průměrná pravděpodobnost poruchy při vyžádání PFD_{SYS} se nahradí pravděpodobností nebezpečné poruchy za hodinu PFH_{SYS} .

Celková pravděpodobnost nebezpečné poruchy bezpečnostní funkce E/E/PE systému PFH_{SYS} se určí výpočtem intenzit nebezpečných poruch všech subsystému společně zajišťující danou bezpečnostní funkci a jejich sečtení a toto můžeme vyjádřit tímto způsobem [6]:

$$PFH_{SYS} = PFH_s + PFH_L + PFH_{FE} \ [-] \tag{12}$$

PFH_{SYS} - pravděpodobnost poruchy za hodinu bezpečnostní funkce pro E/E/PE systému souvisejícího s bezpečností $[-]$

PFH_S - pravděpodobnost poruchy za hodinu subsystému senzorů $[-]$

PFH_L - pravděpodobnost poruchy za hodinu subsystému logiky $[-]$

PFH_{FE} - pravděpodobnost poruchy za hodinu koncových prvků $[-]$

3.6.4 Architektury pro režim provozu s vysokým nebo nepřetržitým vyžádáním

Architektura 1oo1pro režim s vysokým nebo nepřetržitým vyžádáním

Schéma této architektury je na obrázku č. 10 a č. 11.

Intenzita nebezpečných poruch kanálu λ_D [6]:

$$\lambda_D = \lambda_{DU} + \lambda_{DD} = \frac{\lambda}{2} \ [h] \tag{13}$$

Ekvivalentní střední doba prostoje kanálu t_{CE} [6]:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \ [h] \tag{14}$$

Intenzita zjištěných poruch λ_{DU} [6] :

$$\lambda_{DU} = \frac{\lambda}{2} \cdot (1 - DC)\,[h] \tag{15}$$

Intenzita nezjištěných poruch λ_{DD} [6]**:**

$$\lambda_{DD} = \frac{\lambda}{2} \cdot DC\,[h] \tag{16}$$

Průměrná pravděpodobnost poruchy při vyžádání PFH_G, za předpokladu, že bezpečnostní systém nastavuje ECU do bezpečného stavu při zjištění jakékoliv poruchy je platný tento vzorec pro výpočet pravděpodobnosti poruchy pro skupinu kanálů [6]:

$$PFH_G = 2 \cdot \lambda_{DU}\ [-] \tag{17}$$

λ_{DU} - intenzita nezjištěných nebezpečných poruch $[h]$

Architektura 1oo2 pro režim s vysokým nebo nepřetržitým vyžádáním

Tato architektura je stejná jako pro režim s nízkým vyžádáním a je zobrazena na obrázku č. 10 a č. 11. Pro výpočet t_{CE} se použije rovnice (8).

3.7 Sestavování stromů poruchových stavů pro bezpečnostní funkce

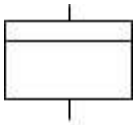
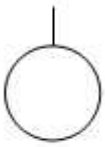
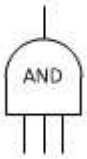
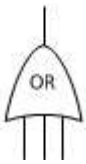
Při sestavování stromu poruchových stavů je nutno nejprve určit vrcholovou událost, od které se odvíjí strom poruchových stavů směrem dolu. Vstupní události, které vstupují do vrcholové události, jsou systematicky rozvíjeny tak, aby vycházely ze svých vstupních událostí.

Každý vstup ve stromu poruchových stavů, který směřuje směrem dolů, se samostatně rozvíjí až do doby, kdy dosáhne základní události.

Při analýze musí být přesně definováno, zda je nutno systém analyzovat až po jednotlivé součásti nebo pouze na úroveň montážních sestav [12].

V tabulce č. 7 jsou uvedené grafické značky, jejich název a popis. Tyto grafické značky spolu s použitím spojnic a popisků slouží k sestavení stromu poruchových stavů

Tabulka č. 7: Grafické značky analýzy stromu poruchových stavů [12]

Značka	Název	Popis
	Blok události	Blok s názvem nebo popisem události
	Základní událost	Základní (primární) událost – událost, která se dále nedělí.
	Hradlo AND	Hradlo AND (a) – událost nastane pouze tehdy, když současně nastanou všechny vstupní události.
	Hradlo OR	Hradlo OR (nebo) – událost nastane tehdy, když nastane kterákoliv vstupní událost, nebo jejich libovolná kombinace

4 Analýza požadavků na integritu bezpečnosti konstrukčních skupin a subsystému vybraného vozidla

V této kapitole provedu analýzu požadavků na integritu bezpečnosti. K analýze jsem zvolil hnací motor, zařízení na předehřev motoru a prostor pro přepravované osoby v městském autobuse Solaris Urbíno 15, který je používán k přepravě osob v DPO a.s. Ostrava.

4.1 Riziková místa a prostory

Sledováním statistických souborů DPO a. s. Ostrava jsem zjistil, že mimo dopravní nehody je cestující nejvíce ohrožen na životě při vzniku požáru vozidla a to hlavně při evakuaci z vozidla při zjištění požáru.

Na vozidlech bylo zaznamenáno několik požárů, které mohly ohrozit životy cestujících nebo řidiče vozidla. Nejčastější příčinou bylo poškození palivového potrubí, které vedlo k úniku nafty a následnému požáru hnacího motoru vozidla. K požárům docházelo nejčastěji v motorovém prostoru, ve kterém je umístěno naftové předehřívací zařízení motoru. Z těchto důvodů bylo při nákupu nových vozidel požadováno, aby ve vozidlech bylo nainstalováno zařízení na identifikaci a potlačení požáru.

Dalším rizikovým místem pro vznik požáru se podle mého sledování mimořádných událostí v posledním roce stává přehřátí brzdového kotouče s následkem zahoření v místě podběhu kola.

4.2 Výběr rizikového subsystému

Z konstrukční skupiny motorového vozidla jsem vybral za nejvíce rizikové místa, mezi které patří motor vozidla a nezávislé teplovodní topení. Tato konstrukční skupina je hlídaná proti vzniku požáru automatickým hasícím systémem pro motor a předehřívací zařízení pro předehřev motoru. Prostor pro cestující je hlídán kouřovým čidlem umístěným ve stropě vozidla v prostoru pro cestující. Prostor kolové jednotky je bez jakéhokoliv zařízení na detekci požáru.

Toto vybrané vozidlo je poháněno naftovým, vznětovým, napříč uloženým motorem od firmy DAF. Hnací moment je přenášen pomocí čtyřstupňové automatické převodovky VOITH DIVA 854.5.

Přes úhlový převod a kardan je krouticí moment přenášen do rozvodovky a pomocí vzestupného redukčního převodu se krouticí moment přenáší do kol zadní nápravy. V pravé zadní části motorového prostoru je umístěno předehřívací zařízení, které slouží k předehřevu chladící soustavy a tím usnadnění startu v zimním období. Vozidlo má tři nápravy. Přední náprava je řídící, druhá náprava je hnací a zadní náprava je vlečená, natáčecí, hydraulicky řízená. Brzdy na všech nápravách jsou kotoučové, automaticky seřizované, ovládané elektropneumaticky. Brzdy jsou vybaveny zařízením EBS.

Obrázek č. 12: Městský autobus Solaris Urbíno 15

Akumulátory jsou umístěny ve schráně na levé straně pod řidičem. Vozidlo používá rozvod o napětí 24 V a ke komunikaci s elektronickým vybavením vozidla je využito CAN vedení, po kterém mezi sebou komunikuji různé elektrické systémy vozidla. V elektrickém rozvodu je použito několik multiplexů, které ovládají ostatní systémy nutné pro provoz vozidla, jako jsou směrovky nebo pérovaní vozidla.

Vozidlo je vypruženo pomocí vzduchových membránových pružin. Vzduch do okruhu pérování dodává elektronicky řízené zařízení ECAS, které hlídá pomocí senzorů výšku vozidla, která je v časových intervalech neustále kalibrována a seřizována do jízdní výšky vozidla.

Vnitřní prostor pro cestující je vybaven 40 místy k sezení, opěrkou v místě pro kočárek nebo invalidní vozík a madly sloužící k držení ve stoje přepravovaných osob, kterých vozidlo pojme až 115. Cestující jsou odbavování pří nástupu nebo výstupu pomocí tří dvoukřídlých širokoprostorných dveří s možností vyžádání otevření dveří při nástupu nebo výstupu.

4.3 Analýza nebezpečí a rizik

Využitím kvalitativní metody odhadu rizika a s použitím diagramu rizika provedu analýzu nebezpečí a rizik pro vznik požáru v prostoru hnacího motoru, prostoru teplovodního topení, vnitřního prostoru pro cestující a kolové jednotky vozidla.

Z výsledků této metody provedu určení jednotlivých úrovní SIL.

K aplikaci tohoto druhu metody zavedu několik potřebných parametrů, které spolu charakterizují vlastnosti nebezpečné situace pro případ selhání některé bezpečnostní funkce daného subsystému. Jde o tyto parametry [5]:

- následku nebezpečné události (C),

- četnosti a době vystavení v nebezpečné oblasti (F),

- možnosti se nebezpečné události vyhnout (P),

- pravděpodobnosti nežádoucího výskytu (W).

Tyto parametry představují rizika a popisují příslušné charakteristiky bezpečnostní funkce daného zařízení.

Po určení úrovně intenzity bezpečnosti SIL a určení bezpečnostních funkcí provedu určení bezpečnostních funkcí a grafické vypracování stromů poruchových stavů pro jednotlivé bezpečnostní funkce.

4.4 Motor vozidla

Motor vozidla je umístěn napříč v zadní části vozidla. Toto umístění nedovoluje řidiči optimální kontrolu z důvodu požáru. Na požár býval řidič upozorněn kouřem, který mohl vysledovat ve zpětném zrcátku, nebo mu byl požár nahlášen cestujícím. Toto opatření je nedostačující, a proto jsou do vozidel instalována automatická zařízení na potlačení požáru.

4.5 Požár v prostoru hnacího motoru

V motorovém prostoru je umístěno detekční vedení naplněné detekční kapalinou pod tlakem 2 MPa. Při vzniku požáru nebo zvýšení okolní teploty na hodnotu 753 °C dojde vlivem teploty k přerušení detekčního potrubí a tím k poklesu tlaku v detekčním potrubí, což má za následek vytlačení hasiva s hasícího válce do hasící větve s tryskami a započetí hašení požáru [7].

Současně je řidič na přístrojové desce vizuálně pomocí kontrolky upozorněn na požár v motorovém prostoru a současně je spuštěn akustický konstantní tón výstražné sirény.

Podle rizikových parametrů provedu určení integrity bezpečnosti SIL při vzniku požáru hnacího motoru vozidla.

Určení rizikového parametru C

Tento rizikový parametr zohledňuje následky nebezpečí při vzniku požáru spalovacího motoru vozidla. Po reakci zařízení na požár a současného rozsvícení kontrolky na přístrojové desce a zaznění výstražného tónu sirény, musí řidič co v nejkratší době podle provozních poměrů a situace kolem vozovky provést zastavení vozidla a zahájit evakuaci cestujících z hořícího vozidla. Evakuace je prováděna přes otevření všech výstupních dveří nebo po rozbití skel nouzových východů pomocí bezpečnostních kladívek, která slouží k usnadnění rozbití skel a jsou umístěna v blízkosti těchto nouzových východů.

Tabulka č. 8: Určení rizikového parametru C [5]

RIZIKOVÝ PARAMETR		KLASIFIKACE
NÁSLEDEK	C1	Menší zranění osob
	C2	Zranění jedné nebo více osob s možností trvalých následků ze zranění nebo možnost smrti jedné osoby
	C3	Smrt několika osob
	C4	Smrt velkého počtu osob

Určení rizikového parametru F

Určení rizikového faktoru F2 jsem provedl na základě určení bezpečnostního systému z hlediska vyžádání bezpečnostní funkce. U systému na potlačení požáru spalovacího motoru jde o systém pracující v provozu s trvalým vyžádáním bezpečnostní funkce. Tento systém tvoří primární ochranu motoru proti vzniku požáru.

Hasicí zařízení je neustále v pohotovostním stavu a dovede uhasit požár i po odstavení vozidla v garážích nebo na odstavném stání.

Tabulka č. 9: Určení rizikového parametru F [5]

RIZIKOVÝ PARAMETR		KLASIFIKACE
Četnost a doba vystavení v nebezpečné oblasti	F1	Vzácné až častější vystavení v nebezpečné oblasti
	F2	Časté až trvalé vystavení v nebezpečné oblasti

Určení rizikového parametru P

Možnost vyhnout se nebezpečné situaci je téměř nemožné. Riziku vzniku požáru se není možno vyhnout. Motor vozidla je sice pod dozorem řidiče, ale z důvodu umístění hnacího motoru vozidla v zadní části, tedy ve velké vzdálenosti od řidiče, jeho selhání nelze vyloučit. Z těchto důvodů volím parametr P_2.

Tabulka č. 10: Určení rizikového parametru P [5]

RIZIKOVÝ PARAMETR		KLASIFIKACE
Možnost se nebezpečné situaci vyhnout	P1	Možné za určitých podmínek
	P2	Téměř nemožné

Určení rizikového parametru W

Pravděpodobnost, že dojde k požáru hnacího motoru je vlivem jeho vylepšené konstrukce málo pravděpodobné, ale není nemožné. Dle statistik a vlastním sledováním vím, že k požáru hnacího motoru občas dochází. Motor je sice pravidelně kontrolován při všech stupních údržby ale některé závady, které vedou ke vzniku požáru nelze běžnými postupy kontroly odhalit a odstranit. Na základě těchto poznatků jsem přiřadil tomuto rizikovému parametru W2, malá pravděpodobnost.

Tabulka č. 11: Určení rizikového parametru W [5]

RIZIKOVÝ PARAMETR		KLASIFIKACE
Pravděpodobnost nežádoucího výskytu	W1	Velmi malá pravděpodobnost
	W2	Malá pravděpodobnost
	W3	Poměrně vysoká pravděpodobnost

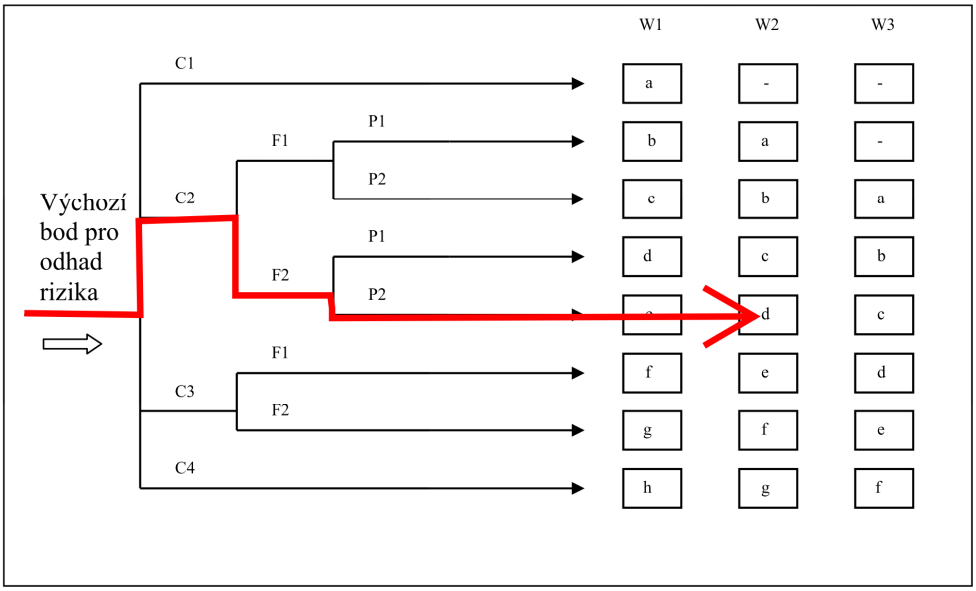
Přehled určených parametrů pro určení SIL

C2 – po zastavení vozidla při evakuaci osob z dopravního prostředku hrozí nebezpečí zranění několika osob nebo může dojít ke smrti evakuované osoby

F2 - časté až trvalé vystavení v nebezpečné oblasti

P2 - téměř nemožné

W2 - malá pravděpodobnost



Obrázek č. 13: Diagram rizika pro BF 1[5]

4.5.1 Přiřazení úrovně integrity bezpečnosti SIL pro hasicí zařízení motoru

Z určených hodnot z tabulek a diagramu rizika jsem přiřadil integritu bezpečnosti zařízení pro potlačení požáru v motorovém prostoru SIL 2 v režimu provozu s trvalým vyžádáním, což znamená, že pravděpodobnost nebezpečných poruch musí být v rozsahu 10^{-6} až 10^{-7}poruch za jednu hodinu [1].

V tabulce č. 12 jsem, provedl popis nebezpečí při požáru vozidla a následky, které by mohli vzniknout při tomto požáru vztažené na přepravované osoby ve vozidle. Určil jsem požadavky na jednotlivé nebezpečné situace a určil bezpečnostní funkce, které slouží ke snížení tohoto nebezpečí.

Tabulka č. 12: Přiřazení úrovně integrity bezpečnosti (SIL) pro zařízení na potlačení požáru hnacího motoru vozidla

Popis nebezpečí	Požadavky na bezpečnost	Následek (C)	Vyžádání funkce (F)	Možnost vyhnutí (P)	Četnost výskytu (W)	SIL
Následek nebezpečí	Opatření ke snížení nebezpečí					
Požár hnacího motoru	Při přítomnosti plamene spustit zařízení na potlačení požáru v prostoru motoru	C2	F2	P2	W2	SIL2
Po zastavení vozidla a při evakuaci osob z dopravního prostředku hrozí nebezpečí zranění několika osob nebo úmrtí osoby	Bezpečnostní funkce číslo 1					

V tabulce č. 13 jsem označenou bezpečnostní funkci stručně popsal a posoudil vliv softwaru na danou bezpečnostní funkci. Nutné je také zajistit, aby zvolené bezpečnostní funkce měla možnost ověření a to buď řidičem vozidla, nebo personálem obstarávající opravy a údržbu vozidla.

Tabulka č. 13: Bezpečnostní funkce zařízení na potlačení požáru hnacího motoru

Označení BF	Popis BF	FTA	Vliv SW	Postup ověření BF
BF 1	Při přítomnosti plamene spustit zařízení na potlačení požáru v prostoru motoru	Obrázek č. 16	NE	Uživatelem provedená kontrola tlaků na manometrech

Jednoduché ověření těchto bezpečnostních funkcí spočívá v provedení kontroly tlakoměru umístěného pod servisním krytem v prostoru u zadních dveří vozidla. Stupnice tlakoměru je rozdělena do tří částí. Střední část označena zelenou barvou potvrzuje funkčnost zařízení na potlačení požáru. Pokud je zjištěno, že tlakoměr ukazuje mimo zelené pole, tlakoměr v červeném poli, je toto vozidlo nezpůsobilé k provozu na pozemních komunikacích a nesmí být použito k přepravě osob. Závadu je nutno vyhledat a odstranit [7].

Obrázek č. 14: Kontrolní manometry na hasícím a detekčním válci

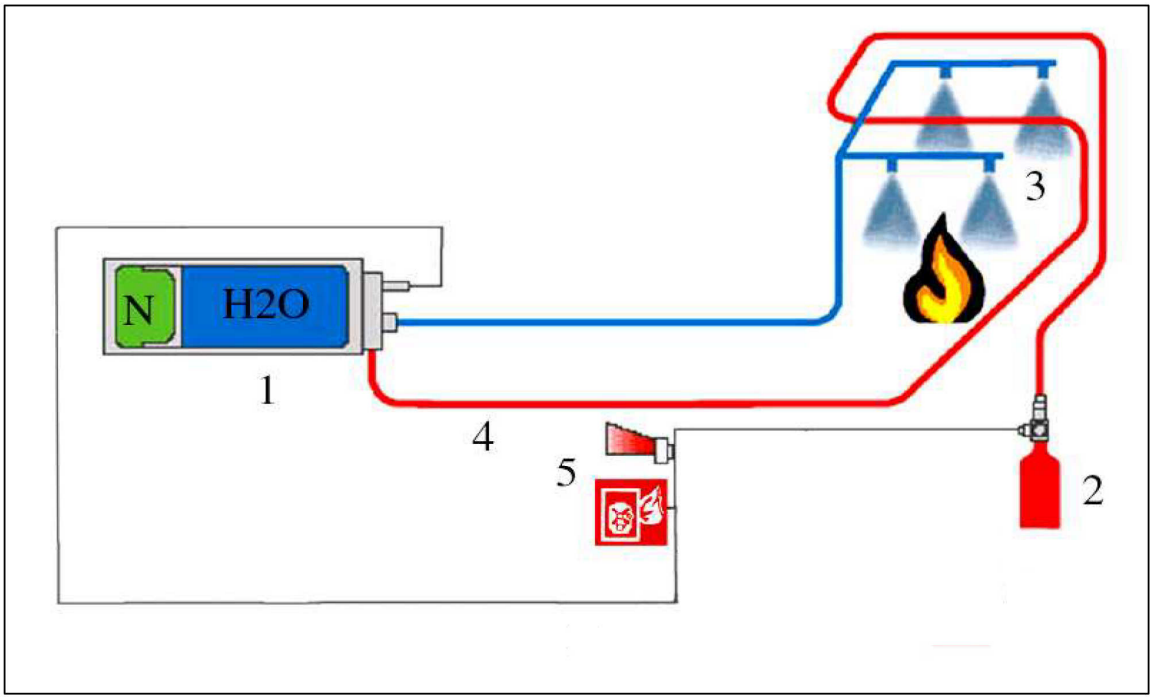
4.6 Automatický hasící systém na potlačení požáru v motorovém prostoru

Autobusy Solaris Urbíno 15 jsou vybaveny plně automatickým hasícím systémem pro motorový prostor a pro přídavné teplovodní vytápění. Systém je aktivován hydropneumaticky a je funkční bez jakéhokoliv napájení.

Při hašení je hasivo rozstřikováno pomocí trysek, které je rozptylováno z kapalné podoby do mraků mlhy ve tvaru sloupců, které snižují teplotu a vytlačují vzduch. Složení hasiva je založeno hlavně na vodě a nemrznoucích přísadách. Běžná doba činnosti zařízení je 3 až 5 sekund a doba účinnosti 50 až 75 sekund [7].

4.6.1 Složení hasicího systému

Systém se skládá s hasícího válce (1) detekčního válce s detekční kapalinou (2), potrubního systému s tryskami (3) detekční hadice s polymeru spojené mezi detekčním válcem a hasícím válcem (4), výstražného světla a bzučáku pro případ požáru nebo nízkého tlaku v detekčním systému (5).



Obrázek č. 15: Schéma hasicího zařízení [7]

1 – hasící válec 2- detekční válec 3 – hasící potrubí s tryskami 4 – detekční hadice
5 – výstražná optická a zvuková signalizace

Detekční hadice a trysky jsou umístěny ve vrchní části motorového prostoru a u přídavného předehřívacího zařízení hasící válec a detekční válec jsou umístěny v samostatném prostoru. Kouřový alarm je umístěn v prostoru cestujících a poplašná signalizace sirény je umístěna v prostoru řidiče. V případě požáru detekční hadice praskne. Při poklesu tlaku v detekčním systému asi na 0,7 MPa, otevře se ventil na hlavním hasícím válci a systémem je aktivován tlakový spínač na detekčním válci, který pošle signál do prostoru řidiče.

Je zde i možnost použít ruční nebo elektrický průraz, který je nainstalován na detekční hadici. Pomocí tohoto průrazu může řidič ručně spustit systém odříznutím detekční hadice.

Hasící válec je natlakován na tlak 10,5 MPa. Pohonná látka obsahuje dusíkový plyn. Tlak lze odečíst na tlakoměru a musí se pohybovat v zeleně vymezeném poli. Hasící válec se dodává se dvěma navzájem připojenými válci. Volitelný je tlakový spínač, který je aktivován, pokud tlak poklesne pod 8,5 MPa.

Hasicí zařízení má bezpečnostní šroub zavěšený na drátku u hlavního válce. Před jakýmkoliv servisním zásahem, montáží, demontáží nebo při přepravě hasicího zařízení je nutné bezpečnostní šroub zasunout do zajišťovacího otvoru. Šroub brání neúmyslné aktivaci hasicího přístroje [7].

4.6.2 Kontrola detekčního válec

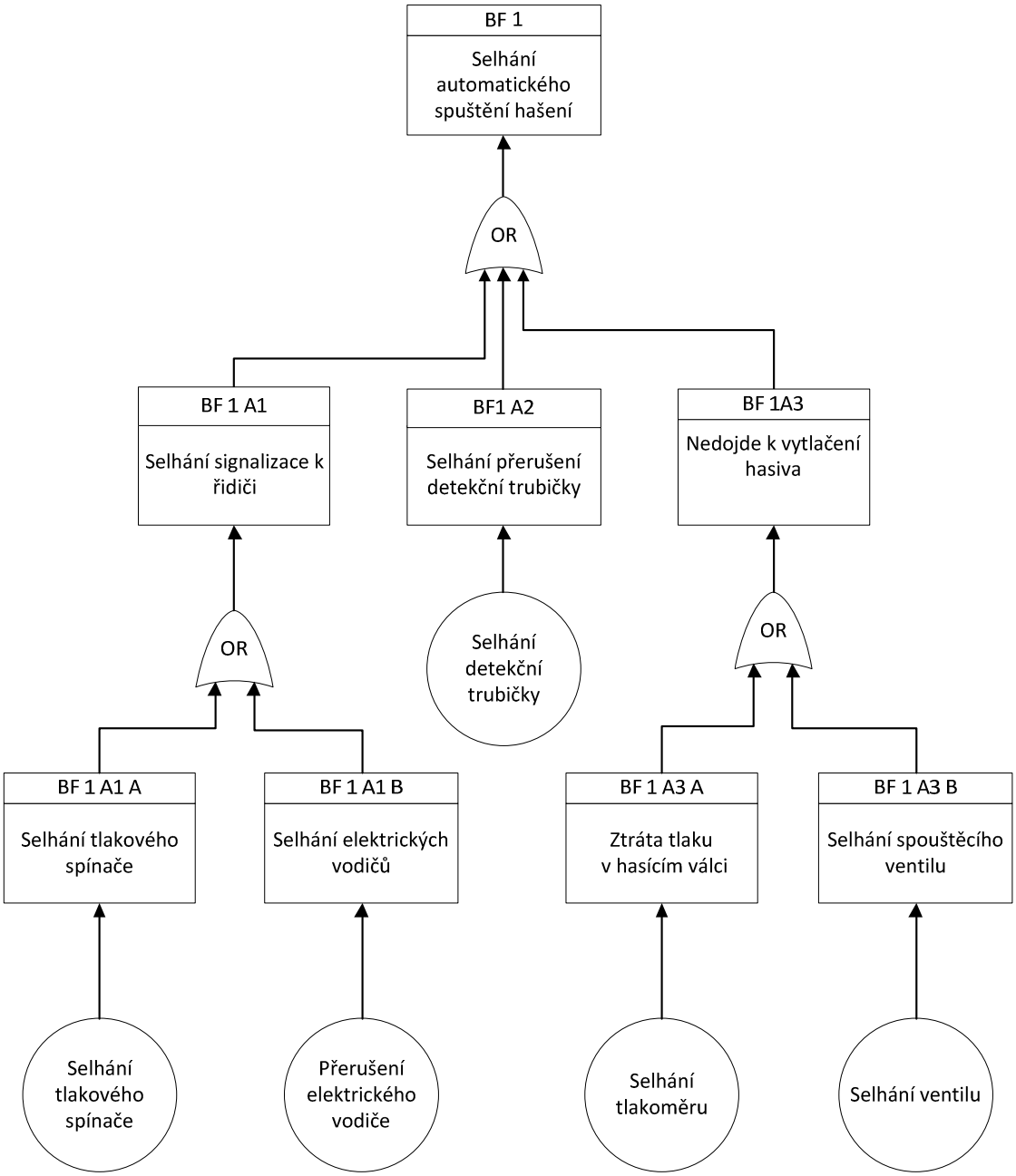
Detekční válec je natlakován detekční kapalinou na tlak 2 MPa. Pohonná látka obsahuje dusíkový plyn. Tlak lze odečíst na tlakoměru a musí se pohybovat v zeleně vymezeném poli. Pokud tlak klesne pod 1,4 MPa, tlakový spínač vyšle poplach stejný jako je poplach pro požár. Detekční válec s dodatečným tlakovým spínačem vyšle poplach, pokud tlak klesne pod 0,5 MPa [7].

4.6.3 Revize a lhůty pro výměny součástí hasicího zařízení

Revize hasicího zařízení se provádějí jednou do roka. Revizi může provést pouze autorizovaná osoba. Každý pátý rok je nutná výměna detekční trubičky spouštěcího obvodu a každý desátý rok je nutno provést výměnu hasícího válce s hasivem a spouštěcí ventil, který je součástí hasícího válce [7].

4.7 Strom poruchových stavů pro BF 1

Této bezpečnostní funkci byla přiřazena integrita SIL 2 v režimu s vysokým vyžádáním. Selhání automatického spuštění hašení pro hnací spalovací motor nastane pří selhání jakékoliv bezpečnostní funkce označené BF 1 A1, BF 1 A2 a BF 1 A3. Jedná se tedy o sériovou soustavu, ve které selhání každého prvku vyvolá ztrátu bezpečnostní funkce.



Obrázek č. 16: Strom poruchových stavů pro BF 1

4.7.1 Selhání signalizace k řidiči

Podle stromu poruch je patrno, že k selhání signalizace k řidiči nastane při selhání tlakového spínače, který má za úkol při poklesu tlaku v detekční trubičce spojit elektrické vedení na kostru vozidla a tím uzavřít elektrický obvod pro kontrolku a akustickou sirénu, která poskytne informaci o požáru. Selhání nastane i při přerušení elektrického vodiče, vlivem působení otřesů při provozu vozidla nebo působením chemické reakce s posypovou solí používanou při zimní údržbě vozovek.

4.7.2 Selhání přerušení detekční trubičky

Za jistých okolností požáru nelze vyloučit, že nedojde k přerušení detekční trubičky a tím k selhání spuštění hasicího zařízení. K selhání může dojít například, když dojde k uvolnění úchytů vedení trubičky a sesunutí mimo detekční prostor určený výrobcem tohoto zařízení.

4.7.3 Nedojde k vytlačení hasiva z hasícího válce

Hasivo se nevytlačí z hasícího válce, pokud dojde ke ztrátě tlaku v tomto válci. Ztráta může být způsobena netěsnostmi tohoto válce hlavně v okolí spouštěcího ventilu, kde je napojeno výtlačné potrubí. Další příčinou jak vidíme na stromu poruchových stavů je selhání spouštěcího ventilu. Tento ventil obsahuje šoupátka a těsnící pryžové prvky, které mohou zapříčinit přidření tohoto šoupátka.

4.8 Požár v prostoru teplovodního předehřívacího zařízení

Požár v prostoru předehřívacího zařízení motoru představuje stejná rizika pro přepravované osoby jako požár hnacího motoru. Potlačení požáru v prostoru naftového předehřívacího zařízení je založeno na stejném principu jako automatické hašení hnacího motoru.

Detekční potrubí je vedeno kritickými místy v blízkosti předehřívacího zařízení motoru a tvoří jednu společnou detekční větev. Jedno zařízení na potlačení požáru hlídá kritické prostory předehřívacího zařízení i hnacího motoru. Při vzniku požáru hasí zařízení na potlačení požáru přes trysky současně motor i toto zařízení.

Vlivem stejného přiřazení rizikových faktorů, které jsem přiřadil požáru hnacího motoru vozidla, mohu požár teplovodního předehřívacího zařízení ohodnotit stejnými hodnotami rizikových faktorů, kterými jsem hodnotil riziko vzniku požáru motoru.

4.8.1 Přiřazení SIL pro hasicí zařízení teplovodního topení

Přehled rizikových faktorů

C2 - po zastavení vozidla při evakuaci osob z dopravního prostředku hrozí

nebezpečí zranění několika osob nebo může dojít ke smrti evakuované osoby

F2 - časté až trvalé vystavení v nebezpečné oblasti

P2 - téměř nemožné

W2 - malá pravděpodobnost

Protože dané zařízení pro potlačení požáru má stejné rizikové faktory, které jsem přiřadil pro nebezpečí vzniku požáru hnacího motoru, byly přiřazeny rizikové faktory i naftovému předehřívacímu zařízení, byla danému zařízení přiřazena integrita bezpečnosti SIL 2, která stanovuje pro tuto funkci pravděpodobnost nebezpečných poruch rozsahu rovno nebo větší 10^{-6} a menší než 10^{-7} poruch za jednu hodinu [1].

Tabulka č. 14: Přiřazení úrovně integrity bezpečnosti (SIL) pro zařízení na potlačení požáru předehřívacího zařízení motoru

Popis nebezpečí	Požadavky na bezpečnost	Následek (C)	Vyžádání funkce (F)	Možnost vyhnutí (P)	Četnost výskytu (W)	SIL
Následek nebezpečí	Opatření ke snížení nebezpečí					
Požár předehřívacího zařízení hnacího motoru	Při přítomnosti plamene spustit zařízení na potlačení požáru v prostoru předehřívacího zařízení	C2	F2	P2	W2	SIL2
Po zastavení vozidla a při evakuaci osob z dopravního prostředku hrozí nebezpečí zranění několika osob nebo úmrtí	Bezpečnostní funkce číslo 2					

Na základě popisu nebezpečí, požadavků, následků a přiřazení úrovně integrity bezpečnosti je opatřením ke snížení nebezpečí realizovaná bezpečnostní funkce číslo 2. Posouzení vlivu software a postup ověření bezpečnostní funkce je uveden v tabulce č. 15.

Tabulka č. 15: Bezpečnostní funkce zařízení na potlačení požáru předehřívacího zařízení motoru

Označení BF	Popis BF	FTA	Vliv SW	Postup ověření BF
BF 2	Při přítomnosti plamene spustit zařízení na potlačení požáru v prostoru předehřívacího zařízení	Obrázek č. 18	NE	Uživatelem provedená kontrola tlaků na manometrech

4.9 Předehřívací zařízení na předehřev motoru

Vozidla jsou vybavena zařízení pro předehřev motoru od firmy Eberspächer. Toto zařízení umožňuje předehřev chladicí kapaliny motoru a touto funkcí usnadňuje spouštění studeného motoru v zimních měsících a v tomto období zajišťuje také tepelný komfort pro cestující. Vozidla jsou vytápěna pomocí teplovodních výměníků, kterým dodává tepelnou energii chladicí kapalina motoru.

4.9.1 Stavba přístroje na předehřev motoru

Přídavný přístroj na předehřev motoru a topného systému vozidla se skládá z těchto částí:

- základní přístroj, který je složen z hořáku s vysokotlakým rozprašováním, výměníku tepla vody, elektrického zařízení (elektronického řídící jednotky),

- díly pro napojení na okruh vody, vodní čerpadlo, vodní termostat, přípojky, kolena, uzavírací ventily,

- díly pro přívod paliva skládající se z palivového potrubí a palivového filtru,

- prvky obsluhy, které přestavuje například universální spínač, spínací hodiny, spínač na uzavíracích ventilech a různé kontrolky k indikaci poruch [8].

4.9.2 Poruchové stavy přístroje na předehřev motoru

Nevytvoření plamene:

Jakmile se otevře magnetický ventil paliva, naběhne takzvaná pojistná doba, která trvá asi deset sekund. Jestliže fotoelektrický odpor v průběhu této doby nenahlásí plamen,

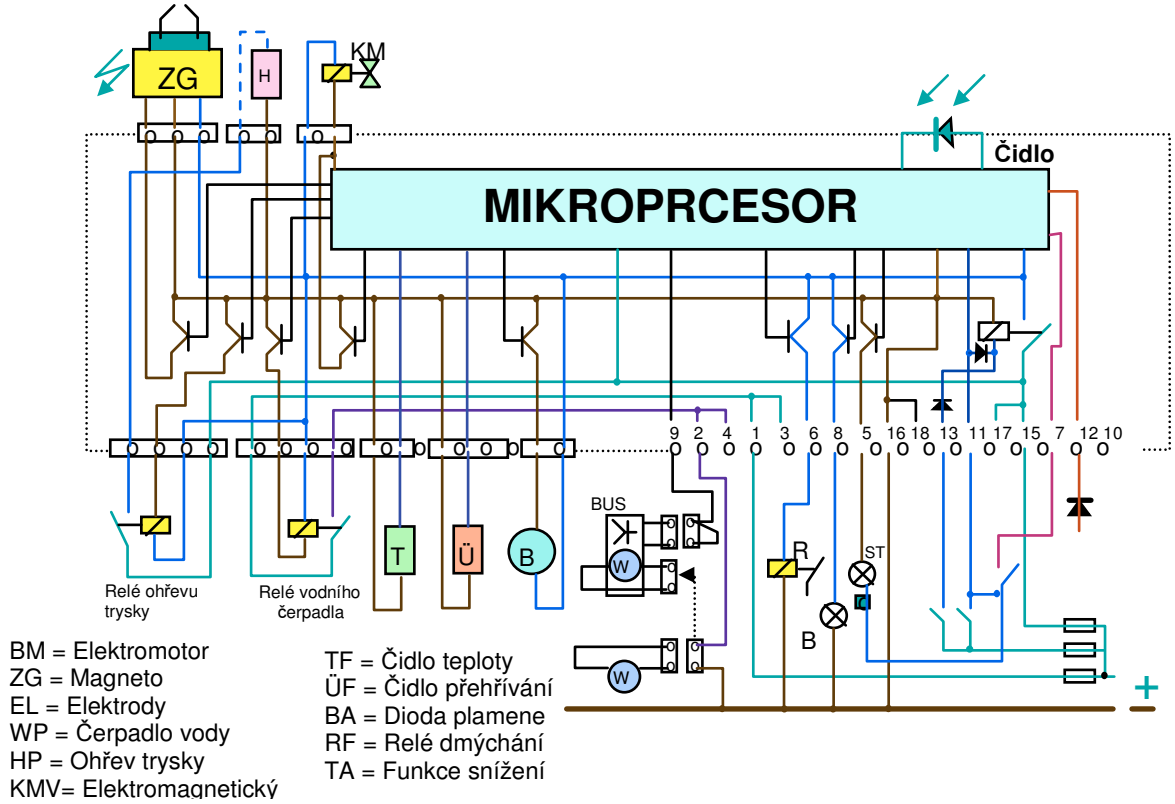
magnetický ventil paliva se ihned uzavře a motor hořáku a vodního čerpadla se po 150 sekundách samočinně vypne.

Zhasnutí plamene:

Jestliže fotoelektrický odpor zaznamená zhasnutí plamene, provede se nový pokus o zapálení a nastartuje se pojistná doba. Je-li tato doba překročena, následuje poruchové vypnutí.

Přehřátí přístroje

Jestliže teplota stoupne na výměníku tepla na nepřístupnou výši, dojde k trvalému vypnutí topení vlivem tavné pojistky reagující na teplotu výměníku tepla [8].

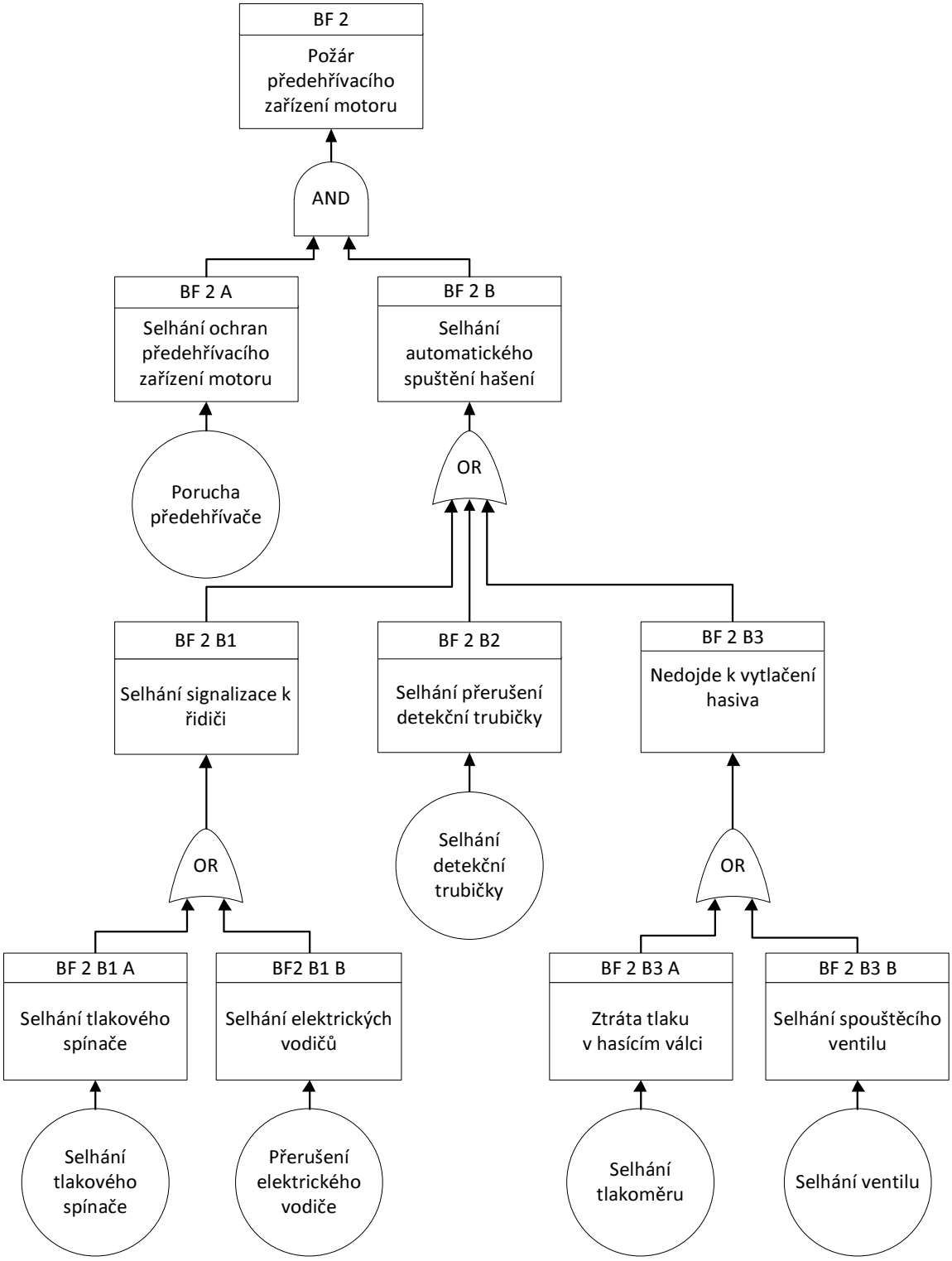


Obrázek č. 17: Schéma zapojení teplovodní přídavné topení [8]

4.10 Strom poruchových stavů pro BP 2

Této bezpečnostní funkci byla přiřazena integrita SIL 2 v režimu s vysokým vyžádáním. Předehřívací zařízení motoru používá k ochraně proti požáru své vlastní bezpečnostní funkce založené na uzavření přívodu paliva do spalovacího zařízení tohoto přístroje pomocí elektromagnetického ventilu.

Selhání BF 2 A nebo BF 2 B nevyvolá selhání BF 2. Ze stromu poruchových stavů vidíme, že se jedná o paralelní soustavu, ve které selhání protipožární ochrany předehřívacího zařízení nevyvolá selhání bezpečnostní funkce automatického spuštění hasicího zařízení.



Obrázek č. 18: Strom poruchových stavů pro BF 2

4.10.1 Selhání ochran předehřívacího zařízení motoru

Základní ochranné prvky tohoto zařízení tvoří fotoodpor, snímač teploty a snímač přehřátí, které pomocí řídící jednotky ovládají elektromagnetický ventil, který uzavírá přívod nafty do spalovacího prostoru tohoto zařízení.

4.10.2 Selhání automatického spuštění hašení

Selhání této bezpečnostní funkce v pravé větvi stromu poruch bude zapříčiněno stejným selháním bezpečnostních funkcí, ke kterým došlo při selhání BF1.

4.11 Požár v prostoru pro cestující

Požár v tomto prostoru ohrožuje bezpečnost přepravovaných osob. Za přítomnosti kouře z požáru zde může vzniknout nepřehledná situace a pří evakuaci osob může dojít k jejich zranění.

K určení úrovně integrity bezpečnosti jsem použil kvantitativní metodu diagramu rizik.

Tabulka č. 16: Přiřazení úrovně integrity bezpečnosti (SIL) pro zařízení na potlačení požáru v prostoru pro cestující

Popis nebezpečí	Požadavky na bezpečnost	Následek (C)	Vyžádání funkce (F)	Možnost vyhnutí (P)	Četnost výskytu (W)	SIL
Následek nebezpečí	Opatření ke snížení nebezpečí					
Požár v prostoru pro cestující	Pří přítomnosti kouře v prostou pro cestující spustit alarm	C1	F2	P2	W2	SIL0
Po zastavení vozidla a při evakuaci osob z dopravního prostředku hrozí nebezpečí zranění několika osob	Není třeba přijímat žádná zvláštní opatření					

Určení rizikového parametru C

Rizikový parametr následku výskytu kouře v prostoru pro cestující zohledňuje následky při spuštění alarmu. Při evakuaci osob z postiženého vozidla je možnost, že dojde ke zranění několika osob. Z těchto důvodů volím rizikový parametr C1.

Určení rizikového parametru F

Zařízení pro detekci kouře v prostoru pro cestující je v neustálé činnosti a monitoruje výskyt kouře v tomto prostoru. Protože toto čidlo kouře plní primární funkci detekce kouře, je zařazeno do vysoké četnosti vyžádání této bezpečnostní funkce. Z tabulky klasifikace parametrů jsem tedy vybral parametr F2.

Určení rizikového parametru P

Parametr určuje možnost se nebezpečné události, tedy selhání zařízení vyhnout, popřípadě zohledňuje skutečnost, že selhání je možno nahradit upozorněním obsluhy, v našem případě řidiče, cestujícím, že v prostoru pro cestující je přítomen kouř z neznámého zdroje. I přes tuto možnost volím klasifikaci P2, protože selhání osoby není možno vyloučit.

Určení rizikového parametru W

Pravděpodobnost, že dojde k výskytu kouře v prostoru pro cestující, není vyloučena. Přiřadil jsem tomuto rizikovému parametru hodnotu W2, která určuje malou pravděpodobnost výskytu této události.

Přehled rizikových parametrů pro určení SIL

C1 – po zastavení vozidla a evakuaci osob z vozidla může dojít ke zranění několika

osob

F2 - časté až trvalé vystavení v nebezpečné oblasti

P1 - téměř nemožné

W2 - malá pravděpodobnost

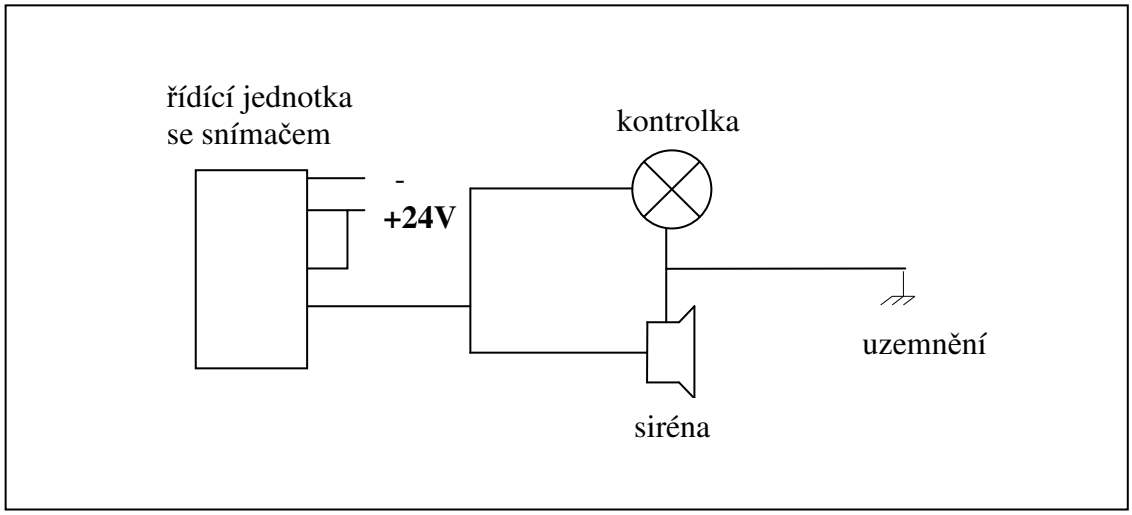
4.11.1 Určení SIL pro detekci kouře v prostoru pro cestující

Z určených hodnot a diagramu rizika jsem zjistil, že k bezpečnostní funkci detekce kouře v prostoru pro cestující není nutno přijímat žádná další bezpečnostní opatření a tato bezpečnostní funkci jsem přiřadil hodnotu bezpečnosti SIL 0.

4.12 Bezpečnostní zařízení v prostoru pro cestující

Ke zvýšení ochrany prostoru pro cestující slouží kouřový detektor Tento detektor je zapojen nezávisle na činnosti zařízení k potlačení vzniku požáru v motorovém prostoru. Zjednodušené schéma vidíme na obrázku č. 19. Bezpečnostní zařízení informuje řidiče o přítomnosti kouře v prostoru pro cestující.

Detektor je umístěn ve stropní části vozidla. Je napájena trvale z napájecí sítě vozidla. Výstražný signál přítomnosti kouře v prostoru pro cestující vydaný snímačem je veden pomocí elektrických vodičů do prostoru přístrojového panelu řidiče, kde je umístěna siréna, která při vzniku kouře vydává nepřetržitý výstražný tón.



Obrázek č. 19: Zjednodušené schéma detektoru kouře [7]

Při aktivaci kouřového čidla dojde současně s akustickým signálem k rozsvícení výstražné kontrolní svítilny umístěné na panelu kontrolek v prostoru řidiče. Povinností řidiče při tomto signálu je co v nejkratším čase provést odstavení vozidla na vhodném místě, ve kterém nedojde k ohrožení bezpečnosti evakuovaných osob, které vozidlo opouštějí.

V následné fázi je povinen provést vizuální kontrolu vozidla a zjistit, z jakých příčin došlo ke spuštění alarmu. V případě zjištění požáru v prostoru hnacího motoru může pomocí ventilu provést ruční spuštění zařízení na potlačení požáru a požár uhasit, nebo k uhašení použít hasicího přístroje, který je součástí povinné výbavy vozidla.

4.13 Požár v prostoru kolové jednotky

Z registru mimořádných událostí v DPO a.s. Ostrava jsem vysledoval, že v posledním roce dochází k nárůstu zahoření v prostoru kolové jednotky. Ve všech případech se jedná o poruchu mechanizmu pro seřízení vzdáleností brzdového kotouče nebo k zadření vodících čepů třmene kotoučové brzdy. Ve všech případech došlo včasným zásahem obsluhy vozidla k uhašení vznikajícího požáru pomocí ručního hasicího přístroje.

4.13.1 Určení SIL pro detekci a signalizaci požáru v prostoru kolové jednotky

K určení integrity bezpečnosti pro vznik požáru v prostoru kolové jednotky bylo použito kvalitativní metody, kde SIL byla určena pomocí diagramu rizik.

Tabulka č. 17: Přiřazení úrovně integrity bezpečnosti pro zařízení na potlačení požáru prostoru kolové jednotky

Popis nebezpečí	Požadavky na bezpečnost	Následek (C)	Vyžádání funkce (F)	Možnost vyhnutí (P)	Četnost výskytu (W)	SIL
Následek nebezpečí	Opatření ke snížení nebezpečí					
Požár v prostoru kotoučové brzdy kola	Pří přítomnosti vysoké teploty informovat o tomto stavu řidiče vozidla	C1	F2	P2	W2	SIL0
Po zastavení vozidla a při evakuaci osob z dopravního prostředku hrozí nebezpečí zranění několika osob	Není třeba přijímat žádná zvláštní opatření					

Určení rizikového parametru C

Rizikovým faktorem následku při požáru kolové jednotky je, že při evakuaci osob z postiženého vozidla je možnost, že dojde ke zranění několika osob. Toto situaci hodnotím parametrem C1.

Určení rizikového parametru F

Snímače teploty kolové jednotky budou umístěny ve štítu rejdového čepu a budou tvořit jedinou bezpečnostní ochranu jednotlivých kolových jednotek. Tento rizikový faktor určuji hodnotou F2, protože toto zařízení bude pracovat v režimu vysokého vyžádání této bezpečnostní funkce.

Určení rizikového parametru P

Možnost vyhnutí se požáru kolové jednotky považuji za téměř nemožnou. Je zde sice možnost, že zkušený řidič rozpozná nestandardní chování vozidla za provozu, které se projeví zvýšeným jízdním odporem nebo negativními silovými účinky na řídící mechanizmus, ale selhání lidského faktoru není možno vyloučit. V těchto případech je nutno volit parametr P2.

Určení rizikového parametru W

Pravděpodobnost, že dojde k požáru kolové jednotky, není vyloučena. Brzdy vozidel jsou pravidelně kontrolovány a opravovány, ale podle statistiky požárů v DPO a.s. Ostrava je možno vysledovat, že k těmto nežádoucím výskytům dochází. Z těchto důvodů hodnotím rizikový parametr hodnotou W2.

Přehled rizikových parametrů pro určení SIL

C1 – po zastavení vozidla a evakuaci osob z vozidla může dojít ke zranění několika

osob

F2 - časté až trvalé vystavení v nebezpečné oblasti

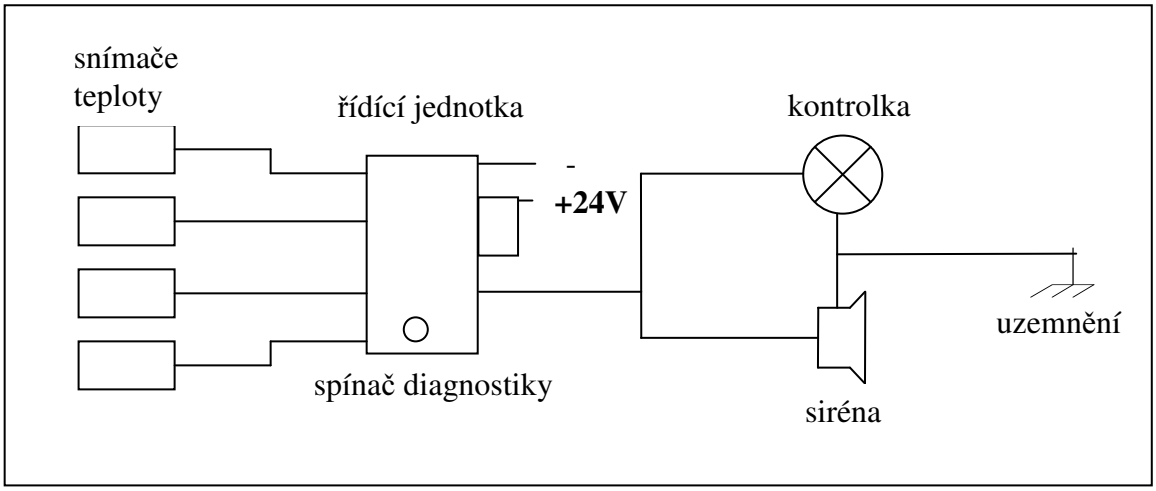
P1 - téměř nemožné

W2 - malá pravděpodobnost

Z určených parametrů rizik a diagramu rizika jsem určil, že u vzniku požáru v prostoru kolové jednotky není nutno přijímat žádná další bezpečnostní opatření. Této bezpečnostní funkci jsem přiřadil hodnotu bezpečnosti SIL 0.

4.14 Návrh bezpečnostního zařízení v prostoru kolové jednotky

Pro zvýšení bezpečnosti přepravovaných osob navrhuji montáž bezpečnostního zařízení, které by v případě vysoké teploty v kolové jednotce informovalo o tomto stavu řidiče vozidla, rozsvícením kontrolky a zazněním zvukového signálu Zjednodušené elektrické schéma zapojení tohoto zařízení je na obrázku č. 20.



Obrázek č. 20: Zjednodušené schéma detektoru zvýšené teploty kolové jednotky

Reakcí řidiče na tuto událost by bylo zastavení vozidla na vhodném místě a provedení evakuace přepravovaných osob. Následovalo by provedení vizuální kontroly všech kolových jednotek, zda se zde nevyskytuje ohnisko požáru a případné uhašení požáru pomocí ručních hasicích přístrojů.

Ke snížení množství nebezpečných nezjištěných poruch tohoto zařízení doporučuji na řídící jednotku nainstalovat diagnostické tlačítko, které po stisknutí ověří snímače teploty a prověří funkci kontrolky a výstražné sirény.

V tabulce č. 18 je uvedeno shrnutí přiřazení integrity bezpečnosti pro všechna zařízení na potlačení požáru, která jsou umístěna ve vybraném vozidle.

Tabulka č. 18: Přiřazení úrovně integrity bezpečnosti (SIL) pro zařízení na potlačení požáru vozidla

P. č.	Popis nebezpečí	Požadavky na bezpečnost	Následek (C)	Vyžádání funkce (F)	Možnost vyhnutí (P)	Četnost výskytu (W)	SIL
	Následek nebezpečí	Opatření ke snížení nebezpečí					
1	Požár hnacího motoru	Při přítomnosti plamene spustit zařízení na potlačení požáru v prostoru motoru	C2	F2	P2	W2	SIL2
	Po zastavení vozidla a při evakuaci osob z dopravního prostředku hrozí nebezpečí zranění několika osob nebo úmrtí	Bezpečnostní funkce číslo 1					
2	Požár předehřívacího zařízení hnacího motoru	Při přítomnosti plamene spustit zařízení na potlačení požáru v prostoru předehřívacího zařízení	C2	F2	P2	W2	SIL2
	Po zastavení vozidla a při evakuaci osob z dopravního prostředku hrozí nebezpečí zranění několika osob nebo úmrtí	Bezpečnostní funkce číslo 2					
3	Požár v prostoru pro cestující	Pří přítomnosti kouře v prostou pro cestující spustit alarm	C1	F2	P2	W2	SIL0
	Po zastavení vozidla a při evakuaci osob z dopravního prostředku hrozí nebezpečí zranění několika osob	Není třeba přijímat žádná zvláštní opatření					
4	Požár v prostoru kotoučové brzdy kola	Pří přítomnosti vysoké teploty informovat o tomto stavu řidiče vozidla	C1	F2	P2	W2	SIL0
	Po zastavení vozidla a při evakuaci osob z dopravního prostředku hrozí nebezpečí zranění několika osob	Není třeba přijímat žádná zvláštní opatření					

5 Orientační výpočet pro ověření cílové míry poruch pro BF 1 a BF 2

Pro tyto výpočty jsem použil metody a postupy doporučené v normě ČSN EN 61 508.

Dle doporučení výrobců jsem určil intervaly do prohlídky jednotlivých prvků, popřípadě do jejich výměny. Určil intenzitu poruch a provedl určení diagnostického pokrytí. Z těchto hodnot jsem vypočetl intenzitu nebezpečných poruch, ze které provedl výpočet pravděpodobnosti poruchy při vyžádání bezpečnostní funkce vybraného koncového prvku ze stromu nebezpečných stavů.

Podle toho zda se jedná o sériovou nebo paralelní soustavu byl proveden výpočet pravděpodobnosti poruchy za hodinu a porovnán, zda splňuje úroveň integrity bezpečnosti pro danou bezpečnostní funkci. Výpočty byly provedeny pomocí aplikace Excel.

5.1 Výpočty pro BF 1

5.1.1 Intervaly kontroly prvků pro BF 1

Interval kontrol T_1 stanovil výrobce zařízení na potlačení požáru na interval jednoho roku. U detekčního vedení je stanovena doba výměny po pěti letech a výměna spouštěcího ventilu je stanovena na deset let.

Tabulka č. 19: Časový interval kontroly a výměny prvků pro BF 1

Součást systému	Interval kontroly [rok]	Interval kontroly T_1 [h]	Poznámka
Tlakový snímač	1	8760	
Tlakoměr	1	8760	
Elektrický vodič	1	8760	
Detekční trubička	5	43800	výměna
Spouštěcí ventil	10	87600	výměna

5.1.2 Diagnostické pokrytí pro BF 1

Diagnostické pokrytí představuje činnost monitorování poruch subsystémem. Jde o poměr míry detekovaných nebezpečných selhání k míře všech nebezpečných selhání. Toto pokrytí lze odvodit podle tabulek v normě ČSN EN 61 508. Je zde i uvedeno, že v případech že tuto hodnotu výrobce neuvádí je možno volit 50% pokrytí. Pro výpočty se používá hodnota v intervalu nula až jedna.

5.1.3 Střední doba prostoje pro BF 1

Střední doba prostoje t_{CE} je doba, po kterou se bude daný prvek soustavy v poruše, ale o této poruše nebudou k dispozici žádné informace.

Vzorec pro výpočet [6]:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \ \ [h] \tag{18}$$

λ_{DU} - intenzita nezjištěných nebezpečných poruch $[h]$

λ_D - intenzita nebezpečných poruch $[h]$

T_1 - interval kontroly $[h]$

$MTTR$ - střední doba do zotavení systému $[h]$

U dopravních prostředků je možno $MTTR$ položit nule, protože po dobu údržby prostředku nehrozí následek nebezpečí při vyžádání této funkce, protože údržba se provádí bez přepravovaných osob.

5.1.4 Intenzita nebezpečných poruch prvku pro BF 1

Hodnota λ_D určuje intenzitu poruch prvku. Jde o hodnotu, která vytváří požadavek na výrobce daného prvku, který by měl splnit, aby bylo dosaženo bezpečnostní funkce na požadované úrovni.

5.1.5 Intenzita nebezpečných nezjištěných poruch pro BF 1

Intenzita nebezpečných poruch λ_{DU} určuje poruchy, které by mohli způsobit ztrátu bezpečnostní funkce. Jedná se o poruchy, které jsou detekovány a také o poruchy které detekovány nejsou. Nejnebezpečnější poruchy pro systém jsou ty, které nejsou detekovaný.

Vzorec pro výpočet [6]:

$$\frac{\lambda_{DU}}{\lambda_D} = 1 - DC \ [-] \tag{19}$$

$$\lambda_{DU} = \lambda_D - (1 - DC) \ [h]$$

λ_{DU} - intenzita nezjištěných nebezpečných poruch $[h]$

λ_D - intenzita nebezpečných poruch $[h]$

DC - diagnostické pokrytí $[-]$

Tabulka č. 20: Vypočtené hodnoty pro BF 1

Součást systému	DC $[-]$	t_{CE} $[h]$	λ_D $[h]$	λ_{DU} $[h]$
Tlakový snímač	0,5	2190	1,00E-06	5,00E-07
Tlakoměr	0,5	2190	1,00E-06	5,00E-07
Elektrický vodič	0	4380	1,00E-06	1,00E-06
Detekční trubička	0,5	10950	1,50E-06	7,50E-07
Spouštěcí ventil	0,5	21900	1,50E-06	7,50E-07

5.1.6 Průměrná pravděpodobnosti poruchy prvku při vyžádání BF 1

Výpočet pravděpodobnosti poruchy prvku vychází z exponenciálního rozdělení $\mathrm{EX}(\lambda)$, které je určeno jedním parametrem λ. Průběh intenzity poruch při tomto rozdělení je konstantní.

Pravděpodobnost poruchy při vyžádání bezpečnostní funkce popisuje distribuční funkce tohoto rozdělení a je dána vztahem [6]:

$$PFD_{SYSp} = 1 - e^{-\lambda_{DU} \cdot t_{CE}} \ [-] \tag{20}$$

PFD_{SYSp} - pravděpodobnost poruchy prvku při vyžádání bezpečnostní funkce $[-]$

λ_{DU} - intenzita nezjištěných nebezpečných poruch $[h]$

t_{CE} - interval periodické kontrolní zkoušky $[h]$

Tabulka č. 21: Průměrná pravděpodobnost poruchy prvku při vyžádání BF 1

Součást systému	PFD_{SYS} $[-]$
Tlakový snímač	1,09E-03
Tlakoměr	1,09E-03
Elektrický vodič	4,37E-03
Detekční trubička	8,18E-03
Spouštěcí ventil	1,63E-02

5.1.7 Průměrná pravděpodobnosti poruchy soustavy při vyžádání BF 1

Ze stromu poruchových stavů je patrno, že u BF 1 jde o sériovou soustavu, ve které porucha kteréhokoliv prvku vyvolá ztrátu bezpečnostní funkce. Pro tuto soustavu platí vztah:

$$PFD_{SYS} = \sum PFD_{SYSp} \ [-] \tag{21}$$

PFD_{SYS} - pravděpodobnost poruchy soustavy při vyžádání bezpečnostní funkce $[-]$

PFD_{SYSp} - pravděpodobnost poruchy prvku při vyžádání bezpečnostní funkce $[-]$

Obrázek č. 21: Řazení prvků základních událostí BF 1

5.1.8 Výpočet pravděpodobnosti nebezpečné poruchy pro BF 1

Výpočet pravděpodobnosti poruchy za hodinu PFH_{SYS} je počítán z PFD_{SYS} a času stanoveného dobou životností vozidla, která je výrobcem stanovena na 12 let. Přepočtem na hodiny je t_{CE} stanoven na 105 120 hodin.

Pro systémy s vysokým nebo nepřetržitým vyžádáním platí vztah [6]:

$$PFH_{SYS} = \frac{PFD_{SYS}}{t_{CE}} \ [-] \tag{22}$$

PFH_{SYS} -pravděpodobnost poruchy za hodinu $[-]$

PFD_{SYS} - pravděpodobnost poruchy při vyžádání bezpečnostní funkce $[-]$

t_{CE} - životnost vozidla $[h]$

5.1.9 Výsledky výpočtů pro BF 1

Výpočty jednotlivých částí BF 1 byly provedeny v tabulkovém procesoru Excel a jsou zobrazeny v tabulce č. 22.

Bezpečnostní funkci BF1 byla přeřazena integrita bezpečnosti SIL 2. Soustava je tvořena prvky, které jsou v sériovém uspořádání. Z tohoto důvodů mají všechny prvky v BF1 stanoveny integritu bezpečnosti SIL 2.

Tabulka č. 22: Přehled výpočtů pro BF 1

Prvek	T_1 $[h]$	DC $[-]$	t_{CE} $[h]$	λ_d $[h]$	λ_{du} $[h]$	PFD_{SYSp} $[-]$
Tlakový snímač	8760	0,5	2190	1,00E-06	5,00E-07	1,09E-03
Tlakoměr	8760	0,5	2190	1,00E-06	5,00E-07	1,09E-03
Elektrický vodič	8760	0	4380	1,00E-06	1,00E-06	4,37E-03
Detekční trubička	43800	0,5	10950	1,50E-06	7,50E-07	8,18E-03
Spouštěcí ventil	87600	0,5	21900	1,50E-06	7,50E-07	1,63E-02
Pro BF 1	PFD_{SYS} $[-]$					3,10E-02
Pro BF 1	PFH_{SYS} $[-]$					2,95E-07

Zařízení pracuje v režimu vysokého vyžádání a přiřazená integrita bezpečnosti pro SIL 2 stanovuje pravděpodobnost nebezpečné poruchy za hodinu na hodnotě rovno nebo větší než $1 \cdot 10^{-7}$ a menší než $1 \cdot 10^{-6}$. Vypočtená hodnota $2{,}95 \cdot 10^{-7}$ dokázala, že při splnění daných hodnot pro BF 1 splňuje požadavek na SIL 2 v režimu vysokého vyžádání bezpečnostní funkce.

5.2 Výpočty pro BF 2

5.2.1 Intervaly kontroly prvků pro BF 2

Mají stejnou hodnotu jako u BF 1. Přibyla zde jen hodnota pro naftové předehřívací zařízení, která je stanovena životností tohoto zařízení.

Tabulka č. 23: Intervaly kontroly prvků BF 2

Součást systému	Interval kontroly [rok]	Interval kontroly T_1 $[h]$	Poznámka
Tlakový snímač	1	8760	
Tlakoměr	1	8760	
Elektrický vodič	1	8760	
Detekční trubička	5	43800	výměna
Spouštěcí ventil	10	87600	výměna
Předehřívací zařízení	12	105120	výměna

5.2.2 Diagnostické pokrytí pro BF 2

Diagnostické pokrytí bude voleno podle doporučení normy ČSN EN 61 508 a bude navýšeno na hodnotu 0,7 z důvodu vlastní diagnostiky, která se provádí před každým spuštěním předehřívacího zařízení.

5.2.3 Střední doba prostoje pro BF 2

Pro výpočet budou stanoveny stejné podmínky jako u BP 1.

Vzorec pro výpočet střední doby prostoje t_{CE} [6]:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D} \cdot \left(\frac{T_1}{2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \ \ [h] \tag{23}$$

λ_{DU} - intenzita nezjištěných nebezpečných poruch $[h]$

λ_D - intenzita nebezpečných poruch $[h]$

T_1 - interval kontroly $[h]$

$MTTR$ - střední doba do zotavení systému $[h]$

5.2.4 Intenzita nebezpečných nezjištěných poruch pro BF 2

Vzorec pro výpočet [6]:

$$\frac{\lambda_{DU}}{\lambda_D} = 1 - DC \ \ [h] \tag{24}$$

$$\lambda_{DU} = \lambda_D - (1 - DC) \ \ [h]$$

λ_{DU} - intenzita nezjištěných nebezpečných poruch $[h]$

λ_D - intenzita nebezpečných poruch $[h]$

DC - diagnostické pokrytí $[-]$

Tabulka č. 24: Vypočtené hodnoty pro BF 2

Součást systému	DC $[-]$	t_{CE} $[h]$	λ_d $[h]$	λ_{DU} $[h]$
Tlakový snímač	0,5	2190	1,00E-06	5,00E-07
Tlakoměr	0,5	2190	1,00E-06	5,00E-07
Elektrický vodič	0	4380	1,00E-06	1,00E-06
Detekční trubička	0,5	10950	1,50E-06	7,50E-07
Spouštěcí ventil	0,5	21900	1,50E-06	7,50E-07
Předehřívací zařízení	0,7	26280	1,00E-05	3,00E-06

5.2.5 Průměrná pravděpodobnost poruchy prvků při vyžádání BF 2

Vzorec pro výpočet [6]:

$$PFD_{SYSp} = 1 - e^{-\lambda_{DU} \cdot t_{CE}} \ [-] \tag{25}$$

PFD_{SYSp} - pravděpodobnost poruchy prvku při vyžádání bezpečnostní funkce $[-]$

λ_{DU} - intenzita nezjištěných nebezpečných poruch $[h]$

t_{CE} - interval periodické kontrolní zkoušky $[h]$

Tabulka č. 25: Průměrná pravděpodobnost poruchy prvků BF 2

Součást systému	PFD_{SYSp} $[-]$
Tlakový snímač	1,09E-03
Tlakoměr	1,09E-03
Elektrický vodič	4,37E-03
Detekční trubička	8,18E-03
Spouštěcí ventil	1,63E-02
Předehřívací zařízení	1,23E-01

5.2.6 Průměrná pravděpodobnost poruchy soustavy při vyžádání BF 2

Ze stromu poruchových stavů je patrno, že u BF 2 jde o sériově paralelní soustavu. Tuto soustavu tvoří sériová větev BF 2 B která spojením větve pro BF 2A vytváří paralelní soustavu BF 2.

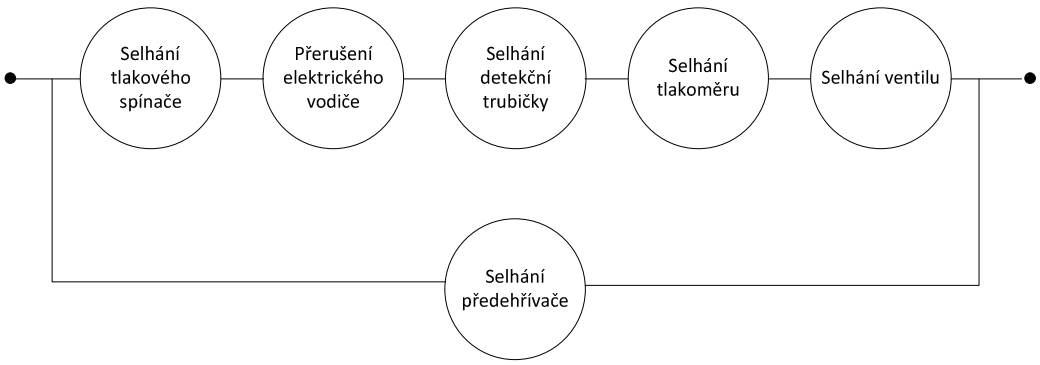
Vzorec pro výpočet:

$$PFD_{SYS} = \sum PFD_{SYSps1} \cdot \sum PFD_{SYSps2} \ [-] \tag{26}$$

PFD_{SYS} - pravděpodobnost poruchy soustavy při vyžádání bezpečnostní funkce $[-]$

PFD_{SYSps1} - pravděpodobnost poruchy při vyžádání bezpečnostní funkce BF 2 A $[-]$

PFD_{SYSps2} - pravděpodobnost poruchy při vyžádání bezpečnostní funkce BF 2 B $[-]$



Obrázek č. 22: Řazení prvků základních událostí BF2

5.2.7 Výpočet pravděpodobnosti poruchy plnit svou funkci pro BF 2

Pro systémy v režimu provozu s nízkým vyžádáním platí vztah [6]:

$$PFH_{SYS} = PFD_{SYS} \ [-] \tag{27}$$

PFH_{SYS} - pravděpodobnost poruchy za hodinu $[-]$

PFD_{SYS} - pravděpodobnost poruchy při vyžádání bezpečnostní funkce $[-]$

5.2.8 Výsledky výpočtů pro BF 2

Bezpečnostní funkci BF2 byla přeřazena integrita bezpečnosti SIL 2. Soustava má ve stromě poruch pod hlavním blokem události umístěno hradlo AND. Událost nad tímto hradlem nastane pouze tehdy, když součastně nastanou všechny vstupní události.

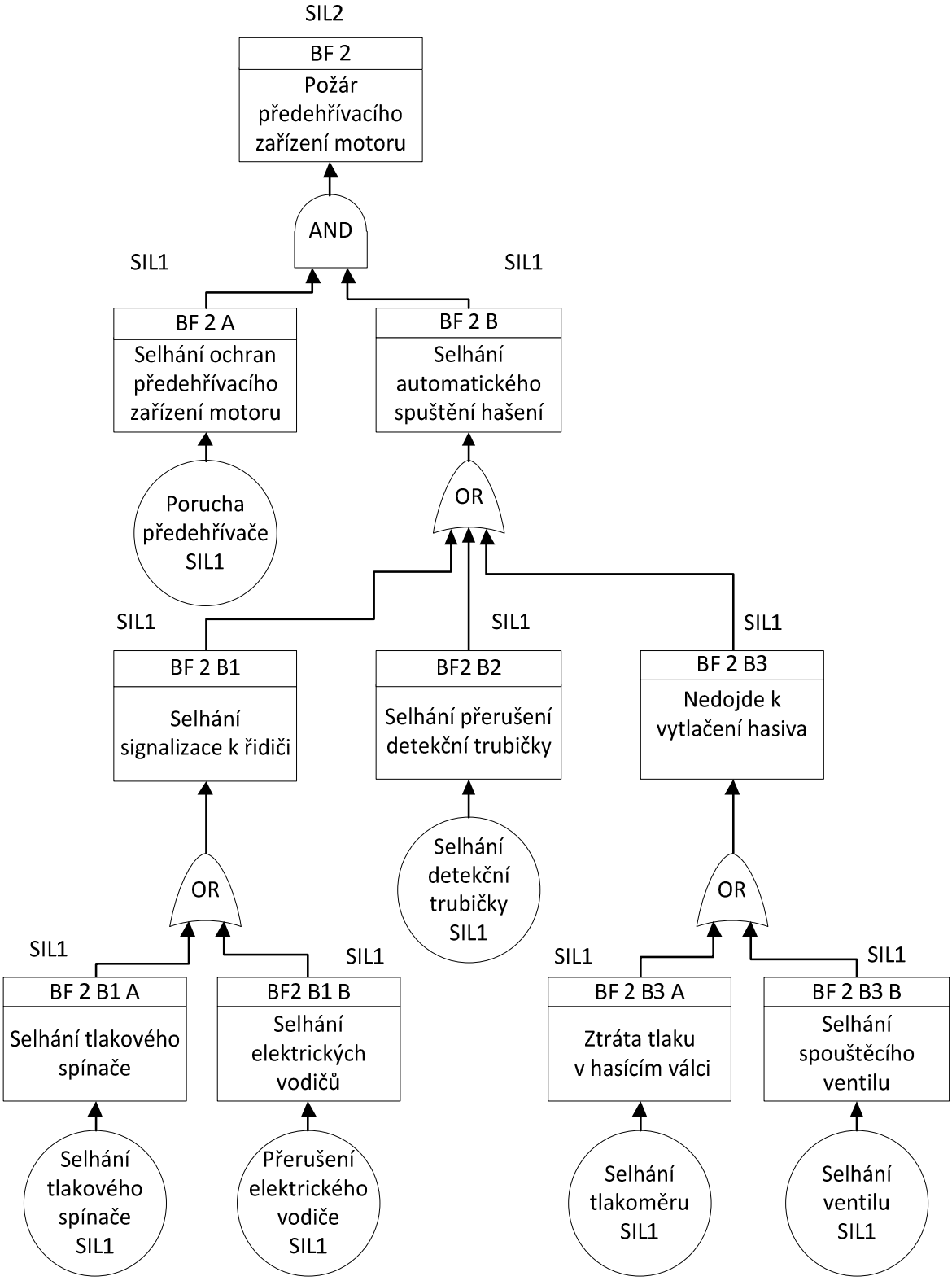
V této sestavě provedu omezení integrity bezpečnosti podle pravidel o omezování, která mi dovolí jednotlivým prvkům v soustavě přiřadit integritu bezpečnosti SIL 1.

Tabulka č. 26: Přehled výpočtů pro BF2

Prvek	T_1 $[h]$	DC $[-]$	t_{CE} $[h]$	λ_d $[h]$	λ_{du} $[h]$	PFD_{SYS} $[-]$
Tlakový snímač	8760	0,5	2190	1,00E-06	5,00E-07	1,09E-03
Tlakoměr	8760	0,5	2190	1,00E-06	5,00E-07	1,09E-03
Elektrický vodič	8760	0	4380	1,00E-06	1,00E-06	4,37E-03
Detekční trubička	43800	0,5	10950	1,50E-06	7,50E-07	8,18E-03
Spouštěcí ventil	87600	0,5	21900	1,50E-06	7,50E-07	1,63E-02
Předehřívací zařízení	105120	0,7	26280	1,00E-05	3,00E-06	4,62E-01
Pro BF 2 A	PFD_{SYS}					3,10E-02
Pro BF 2 B	PFD_{SYS}					1,23E-01
Pro BF 2	PFD_{SYS}					1,43E-03
Pro BF 2	PFH_{SYS}					1,43E-03

Zařízení na potlačení požáru pracuje v režimu vysokého vyžádání a přiřazená integrita bezpečnosti vlivem použití povoleného omezení integrity bezpečnosti pro paralelní soustavu umožnila přiřazení úrovně integrity bezpečnosti SIL 1 u všech základních událostí v obou větvích stromu poruchových stavů BF 2. Předehřívací zařízení motoru má svou vlastní ochranu proti vzniku požáru tvořenou elektroventilem na uzavření paliva do spalovacího prostoru při vzniku poruchového stavu.

Zařízení na potlačení požáru v prostoru motoru a předehřívacího zařízení tvoří až druhou ochrannou vrstvu předehřívacího zařízení motoru. Z těchto důvodů je možno BF 2 překvalifikovat a přiřadit úroveň integrity SIL 2 s režimem provozu s nízkým vyžádáním [2]. Hodnota střední pravděpodobnosti poruchy plnit svou bezpečnostní funkci je pro SIL 2 určena hodnotou rovno nebo větší než $1 \cdot 10^{-3}$ a menší než $1 \cdot 10^{-2}$. Vypočtená hodnota $1{,}43 \cdot 10^{-3}$ dokazuje, že při splnění zadaných hodnot BF 2 splňuje požadavek na SIL 2 v režimu s nízkým vyžádáním bezpečnostní funkce.



Obrázek č. 23: Přiřazení SIL po omezení architektury systému pro BF 2

6 Závěr

Proces posouzení rizika tvoří základ při vývoji požadavků na funkční bezpečnost. Funkční bezpečnost klade vysoké nároky na spolehlivost komponentů jednotlivých funkčních celků zařízení, a tímto dokáže zabránit možnosti poranění nebo smrti osob, ohrožení životního prostředí nebo zamezí vzniku velkých materiálních a finančních ztrát.

Pro přepravované osoby je požár dopravního prostředku nebezpečná událost, která ohrožuje jejich zdraví a životy. Aby bylo možno toto nebezpečí omezit na nejmenší možnou míru, musí provozovatel vozidla rozumět tomu, jak se bezpečnostní systém chová při vzniku jeho poruchy. Analýzu sem provedl pomocí stromu poruchových stavů bezpečnostní funkce. Tato analýza odhalila chyby, které lze detekovat při údržbě tohoto zařízení bez vynaložení nepřiměřených ekonomických nákladů. Pravděpodobnost, že k těmto chybám dojde, může být při použití vhodné konstrukce jednotlivých prvků bezpečnostního systému a zlepšení diagnostických metod, velmi nízká.

Zlepšení funkční bezpečnosti se ve většině případů zajišťuje použitím několika ochranných vrstev systémů, které tvoří celkovou sestavu související s bezpečností. Toto je patrné u bezpečnostní funkce při vzniku požáru předehřívacího zařízení, kde do ochrany před požárem vstupují dvě ochranné vrstvy. První ochrannou vrstvou je zařízení pro potlačení požáru samostatného předehřívacího zařízení, které tvoří fotoodpor a teplotní čidlo, které při selhání bezpečné funkce tohoto zařízení uzavře pomocí elektrického ventilu přívod paliva a vyřadí zařízení z provozu. Druhou vrstvu zajišťuje hasicí zařízení na potlačení požáru v prostoru, ve kterém je umístěno toto předehřívací zařízení.

Výhoda zdvojování funkcí, takzvaného zálohování, dovede také snížit výskyt nebezpečných nediagnostikovaných závad. Zdvojením některých snímačů anebo bezpečnostních komponentů docílíme zvýšení rozsahu hlídaného prostoru a zároveň tím snížíme možnost jejich selhání.

K přidělení integrity bezpečnosti sem použil diagram rizika, který využívá k určení SIL kvalitativní metodu. Podle doby kontroly, výměny nebo životnosti prvků bezpečnostních zařízení jsem provedl výpočet pomocí určených vzorců pro pravděpodobnost nebezpečné poruchy za hodinu, které mi určilo konečnou hodnotu průměrné pravděpodobnosti poruchy při vyžádání bezpečnostní funkce. Tuto hodnotu jsem ověřil, zda splňuje požadavky přiřazené integrity bezpečnosti podle normy ČSN EN 61 508. U obou bezpečnostních funkcí byly tyto požadavky splněny.

Výsledky práce mohou být využity pro stanovení integrity bezpečnosti na další konstrukční celky vozidla nebo pro stanovení požadavků na výrobce, kteří budou vyrábět tato bezpečnostní zařízení, nebo budou dodávat náhradní komponenty do těchto zařízení.

Zájem o analýzu funkční bezpečnosti bude vzrůstat, protože představuje budoucnost v oblasti bezpečnosti strojů. Umožní větší flexibilitu a použití nových technologií již při návrhu a konstrukci nových strojních a dopravních zařízení, nebo také v průběhu celého životního cyklu daného zařízení.

7 Seznam použité literatury

[1] ČSN EN 61 508-1: Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností. Část 1: Všeobecné požadavky. Praha: Český normalizační institut, 2002, 60 s.

[2] ČSN EN 61 508-2: Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností. Část 2: Požadavky na elektrické/elektronické/programovatelné elektronické systémy související s bezpečností. Praha: Český normalizační institut, 2002, 76 s.

[3] ČSN EN 61 508-3: Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností. Část 3: Požadavky na software. Praha: Český normalizační institut, 2002, 52 s.

[4] ČSN EN 61 508-4: Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností. Část 4: Definice a zkratky. Praha: Český normalizační institut, 2002, 32 s.

[5] ČSN EN 61 508-5: Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností. Část 5: Příklady metod určování úrovní integrity bezpečnosti. Praha: Český normalizační institut, 2002, 32 s.

[6] ČSN EN 61 508-6: Funkční bezpečnost elektrických/elektronických/programovatelných elektronických systémů souvisejících s bezpečností. Část 6: Metodické pokyny pro použití. Praha: Český normalizační institut, 2002, 72 s.

[7] Hasící systémy pro motorové prostory, příručka pro řidiče, vydání 2009.

[8] Dílenská příručka pro údržbu a opravy teplovodního topení Eberspächer D 30 W.

[9] UHER, Jaromír. Úvod do funkční bezpečnosti I: norma ČSN EN 61 508. Automa [online], 2004, s. 8-9. Dostupný na WWW: http://www.odbornecasopisy.cz/index.php?id_document=32520.

[10] Babinec, František. K úrovni funkční bezpečnosti. Automa [online], 2008, s. 8-11. Dostupný na WWW: http://www.odbornecasopisy.cz/res/pdf/37395.pdf.

[11] Funkční bezpečnost podle IEC/EN 61 508: Normy – fakta - pozadí. Profess - Info [online]. Dostupný na WWW: http://www.profess.sk/pdf_pci_info/INFO-SIL.pdf.

[12] Holub R., Vintr Z., Spolehlivost letadlové techniky. VUT Brno, 2001. 233 s. [online]. Dostupný na WWW: http://lu.fme.vutbr.cz/files/SpolehlivostLetadloveTechniky.pdf.

[13] Hasicí zařízení s vodní mlhou, [online]. Dostupný na WWW: http://www.fogmaker.cz/index.html.

[14] Funkční bezpečnost podle IEC/EN 61 508: Normy – fakta - pozadí. Profess - Info [online]. Dostupný na WWW: http://www.profess.sk/pdf_pci_info/INFO-SIL.pdf.

[15] Safebook 3, Bezpečnostní řídicí systémy pro stroje a zařízení, [online]. Dostupný na WWW:http://samplecode.rockwellautomation.com/idc/groups/literature/ documents/rm/safebk-rm002_-cs-p.pdf.

8 Seznam obrázků a tabulek

Obrázky:

Tabulky:

9 Seznam příloh

Příloha A: Zapojení detekčního systému zařízení na potlačení požáru [7]

Příloha B: Kontrolní a výstražné nálepky na hasícím válci hasicího zařízení [7]

Příloha C: Zápis o provedení roční kontroly hasícího systému na vozidle

Příloha D: Montážní prvky pro kouřový alarm pro zjištění přítomnosti kouře v prostoru pro cestující [7]